

【特許請求の範囲】

【請求項1】 利用者端末と通信路を介して接続された販売店サーバと、前記利用者端末及び前記販売店サーバと通信路を介して接続された決済サーバとを使用して電子決済を行う電子決済方法であって、

前記販売店サーバが、前記利用者端末から送信される物品若しくはサービスの注文要求を受信するステップと、前記販売店サーバが、前記注文要求に関する決済処理の依頼を前記決済サーバに第1の決済要求として送信するステップと、

前記決済サーバが、前記第1の決済要求の受信と前後して、前記利用者端末から前記注文要求を行った注文に関する決済処理の依頼を第2の決済要求として受信するステップと、

前記決済サーバが、前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に決済処理を行う決済処理ステップとを備えたことを特徴とする電子決済方法。

【請求項2】 前記決済処理ステップが、金融機関によって管理される金融機関ホストマシンと連携して当該決済要求を処理する連携決済ステップを備え、この連携決済ステップに続いて、

前記決済サーバが、前記決済処理結果を利用者端末及び販売店サーバに直接又は間接に送信する決済結果送信ステップとを備えたことを特徴とする請求項1期際の電子決済方法。

【請求項3】 前記決済処理ステップが、前記注文要求の注文内容又は金額が不一致の場合には当該決済処理を不成立とさせる決済不成立ステップを備えたことを特徴とする請求項1又は2記載の電子決済方法。

【請求項4】 通信路で相互に接続された利用者端末、販売店サーバ、決済サーバとを備え、さらに前記決済サーバは、金融機関ホストマシンと接続され、

前記利用者端末が、利用者の操作に応じて前記通信路を用いて前記販売店サーバに物品もしくはサービスの注文要求を送るステップと、

前記販売店サーバが、前記注文要求を受け付けると、前記決済サーバに第1の決済要求を送るステップと、前記利用者端末に支払処理要求を送るステップと、

前記利用者端末が、前記支払処理要求を受け取り、第2の決済要求を前記決済サーバに送るステップと、

前記決済サーバが、前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう決済処理ステップと、

当該決済サーバが、前記決済処理の結果を前記利用者端末に送るステップと、

前記利用者端末が、前記決済処理結果を受け取ると、前記利用者端末から前記販売店サーバに決済処理結果を送るステップと、

前記販売店サーバが、前記決済処理結果を受け取るステップと、を備えたことを特徴とする電子決済方法。

【請求項5】 通信路で相互に接続された利用者端末、販売店サーバ、決済サーバとを備え、この決済サーバは、金融機関ホストマシンと接続され、

10 前記利用者端末が、前記利用者の操作に応じて前記通信路を用いて前記販売店サーバに物品もしくはサービスの注文要求を送るステップと、

前記販売店サーバが、前記注文要求を受け付けると、前記決済サーバに第1の決済要求を送るステップと、前記利用者端末に支払処理要求を送信するステップと、

前記利用者端末が、前記支払処理要求を受け取り、第2の決済要求を前記決済サーバに送るステップと、

前記決済サーバが、前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう決済処理ステップと、

20 前記決済サーバが、前記決済処理の結果を前記販売店サーバに送るステップと、

前記販売店サーバが、前記決済処理結果を受け取るステップと、

前記決済サーバが、前記決済処理の結果を前記利用者端末に送るステップと、

前記利用者端末が、前記決済処理結果を受け取るステップと、を備えたことを特徴とする電子決済方法。

30 【請求項6】 通信路で相互に接続された利用者端末、販売店サーバ、決済サーバとを備え、この決済サーバは、金融機関ホストマシンと接続され、

前記利用者端末が、利用者の操作に応じて前記通信路を用いて前記販売店サーバに物品もしくはサービスの注文要求を送るステップと、

前記販売店サーバが、前記注文要求を受け付けると、前記決済サーバに第1の決済要求を送るステップと、前記利用者端末に支払処理要求を送信するステップと、

40 前記利用者端末が、前記支払処理要求を受け取り、第2の決済要求を前記決済サーバに送信するステップと、

前記決済サーバが、前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう決済処理ステップと、

前記決済サーバが、前記決済処理の結果を前記利用者端末に送るステップと、

前記利用者端末が、前記決済処理結果を受け取るステップと、

50 前記販売店サーバは、前記決済処理の結果を前記決済サ

サーバに問い合わせるステップと、

前記問い合わせを受けた前記決済サーバは、前記販売店サーバに前記決済処理の結果を返すステップと、前記販売店サーバが、前記決済処理の結果を受け取るステップと、を備えたことを特徴とする電子決済方法。

【請求項7】 前記販売店サーバと前記決済サーバとで予め認証子の生成と検証を行なうための鍵を取り交わしておき、

前記決済サーバは、前記認証子生成用の鍵を用いて前記決済処理結果に対する認証子を生成し、前記利用者端末に送る前記決済処理結果に含ませ、

前記利用者端末は、前記決済処理結果を受け取り、前記販売店サーバに送る決済処理結果に前記認証子を含ませ、

前記販売店サーバは、前記決済処理結果を受け取り、前記決済処理結果に含まれる前記認証子と前記認証子検証用の鍵を用いて、前記決済処理結果の認証を行なうことを特徴とする請求項4記載の電子決済方法。

【請求項8】 前記販売店サーバと前記決済サーバの間の通信に、認証可能な通信方法を用い、前記第1の決済要求の送受信において、前記認証可能な通信方法により、前記決済サーバと前記販売店サーバとの相互の認証を行なうことを特徴とする請求項4又は7記載の電子決済方法。

【請求項9】 前記販売店サーバと前記決済サーバの間の通信に、認証可能な通信方法を用い、前記第1の決済要求の送受信および前記決済処理結果の送受信において、前記認証可能な通信方法により、前記決済サーバと前記販売店サーバとの相互の認証を行なうことを特徴とする請求項5又は6記載の電子決済方法。

【請求項10】 前記利用者と前記決済サーバとで予め認証子の生成と検証を行なうための鍵と、前記利用者を識別する利用者識別子とを取り決めておき、

前記利用者端末は、前記認証子生成用の鍵を用いて前記第2の決済要求に対する認証子を生成し、前記認証子と前記利用者識別子を前記第2の決済要求に含ませ、

前記決済サーバは、前記決済処理ステップにおいて、前記第2の決済要求に含まれる前記利用者識別子から前記認証子検証用の鍵を特定し、前記認証子と前記認証子検証用の鍵により、前記利用者および前記第2の決済要求の認証を行なうことを特徴とする請求項4乃至9いずれか一記載の電子決済方法。

【請求項11】 前記利用者と前記決済サーバとで予め認証子の生成と検証を行なうための鍵を取り交わしておき、

前記決済サーバは、前記認証子生成用の鍵を用いて前記決済処理の結果に対する認証子を生成し、前記決済処理の結果に含ませ、

前記利用者端末は、前記決済処理結果を受け取るステップにおいて、前記決済処理の結果に対する認証子と前記

認証子検証用の鍵により、前記決済サーバと前記決済処理結果の認証を行なうことを特徴とする請求項4乃至10いずれか一記載の電子決済方法。

【請求項12】 前記利用者端末と前記決済サーバの間の通信に、認証可能な通信方法を用い、前記第2の決済要求と前記決済処理の結果の送受信において、前記認証可能な通信方法により、前記利用者と決済サーバとの相互の認証を行なうことを特徴とする請求項4乃至9いずれか一記載の電子決済方法。

10 【請求項13】 予め前記利用者と前記決済サーバ間で利用者識別子と利用者秘密情報を取り決め、前記第2の決済要求に、前記利用者識別子と前記利用者秘密情報を含み、

前記決済サーバは、前記決済処理ステップにおいて、前記利用者識別子と前記利用者秘密情報により、利用者の認証を行なうことを特徴とする請求項4乃至9いずれか一記載の電子決済方法。

20 【請求項14】 決済処理に必要な利用者口座情報を前記第2の決済要求に含め、前記利用者口座情報を用いて前記決済サーバが決済処理を行なうことを特徴とする請求項6乃至13いずれか一記載の電子決済方法。

【請求項15】 決済処理に必要な利用者口座情報を前記決済サーバで保持しておき、前記決済サーバは、前記利用者認証が成功した場合に、保持した前記利用者口座情報により決済処理を行なうことを特徴とする請求項10、12又は13記載の電子決済方法。

30 【請求項16】 利用者端末および決済サーバと通信路で接続され、前記利用者端末から注文要求を受け付けると、前記注文内容および決済要求金額に関する情報を含む第1の決済要求を前記決済サーバに送る手段と、

前記利用者端末に前記注文内容および前記決済要求金額に関する情報を含む支払処理要求を送る手段と、前記利用者端末から返される決済処理結果を受け取る手段と、を備えたことを特徴とする販売店サーバ。

40 【請求項17】 利用者端末および決済サーバと通信路で接続され、前記利用者端末から注文要求を受け付けると、前記注文内容および決済要求金額に関する情報を含む第1の決済要求を前記決済サーバに送る手段と、

さらに前記利用者端末に前記注文内容および前記決済要求金額に関する情報を含む支払処理要求を送る手段と、前記決済サーバから返される決済処理結果を受け取る手段と、を含むことを特徴とする販売店サーバ。

50 【請求項18】 利用者端末および決済サーバと通信路で接続され、前記利用者端末から注文要求を受け付けると、前記注文内容および決済要求金額に関する情報を含む第1の決済要求を前記決済サーバに送る手段と、

さらに前記利用者端末に前記注文内容および前記決済要求金額に関する情報を含む支払処理要求を送る手段と、前記第1の決済要求の結果を前記決済サーバに問い合わせる手段と、

前記決済サーバから返される決済処理結果を受け取る手段と、を含むことを特徴とする販売店サーバ。

【請求項19】 前記決済サーバと予め認証子の生成と検証を行なうための鍵を取り交わしておき、前記決済処理結果に含まれる決済処理結果に対する前記決済サーバの認証子と前記認証子検証用の鍵により、前記決済サーバと前記決済処理結果の認証とを行なうことを特徴とする請求項16記載の販売店サーバ。

【請求項20】 前記決済サーバとの間の通信に認証可能な通信方法を用い、

前記第1の決済要求の送受信および前記決済処理結果の送受信において、前記認証可能な通信方法により、前記決済サーバと前記販売店サーバとの相互の認証を行なうことを特徴とする請求項16乃至18いずれか一記載の販売店サーバ。

【請求項21】 利用者端末および販売店サーバと通信路で接続され、さらに金融機関ホストマシンと接続され、

前記販売店から第1の決済要求を受け取る手段と、前記利用者端末から第2の決済要求を受け取る手段と、前記第1の決済要求と前記第2の決済要求とにおける決済内容を照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう手段と、前記決済処理の結果を前記利用者端末に送る手段と、を備えたことを特徴とする決済サーバ。

【請求項22】 利用者端末および販売店サーバと通信路で接続され、さらに金融機関ホストマシンと接続され、

前記販売店から第1の決済要求を受け取る手段と、前記利用者端末から第2の決済要求を受け取る手段と、前記第1の決済要求と前記第2の決済要求とにおける決済内容を照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう手段と、前記決済処理の結果を前記利用者端末に送る手段と、さらに前記決済処理結果を前記販売店サーバに送る手段と、を含むことを特徴とする決済サーバ。

【請求項23】 利用者端末および販売店サーバと通信路で接続され、さらに金融機関ホストマシンと接続され、

前記販売店から第1の決済要求を受け取る手段と、前記利用者端末から第2の決済要求を受け取る手段と、前記第1の決済要求と前記第2の決済要求とにおける決済内容を照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう手段と、前記決済処理の結果を前記利用者端末に送る手段と、前記販売店サーバから前記第1の決済要求の結果の問い合わせを受ける

合わせを受けると、前記販売店サーバに前記決済処理結果を返す手段と、を含むことを特徴とする決済サーバ。

【請求項24】 前記販売店サーバと予め認証子の生成と検証を行なうための鍵を取り交わしておき、前記認証子生成用の鍵を用いて前記決済処理結果に対する前記決済サーバの認証子を生成し、前記決済処理の結果に含めることを特徴とする請求項21記載の決済サーバ。

【請求項25】 前記販売店サーバとの通信に認証可能な通信方法を用い、

前記第1の決済要求の送受信において、前記認証可能な通信方法により、前記販売店サーバの認証を行なうことを特徴とする請求項21又は24記載の決済サーバ。

【請求項26】 前記販売店サーバとの通信に認証可能な通信方法を用い、

前記第1の決済要求の送受信および前記決済処理結果の送受信において、前記認証可能な通信方法により、前記販売店サーバの認証を行なうことを特徴とする請求項22又は23記載の決済サーバ。

【請求項27】 前記利用者と予め認証子の生成と検証を行なうための鍵と、前記利用者を識別する利用者識別子とを取り決めておき、前記決済処理機能において、前記第2の決済要求に含まれる前記利用者識別子から前記認証子検証用の鍵を特定し、前記第2の決済要求に含まれる認証子と前記認証子検証用の鍵により利用者および決済要求の認証を行なうことを特徴とする請求項21乃至26いずれか一記載の決済サーバ。

【請求項28】 前記利用者と予め認証子の生成と検証を行なうための鍵を取り交わしておき、前記認証子生成用の鍵を用いて前記決済処理の結果に対する認証子を生成し、前記決済処理の結果に含めることを特徴とする請求項21乃至27いずれか一記載の決済サーバ。

【請求項29】 前記利用者端末と前記決済サーバとの間の通信に、認証可能な通信方法を用い、前記第2の決済要求と前記決済処理の結果の送受信において、前記認証可能な通信方法により、前記決済サーバと前記利用者との相互の認証を行なうことを特徴とする請求項21乃至28いずれか一記載の決済サーバ。

【請求項30】 予め前記利用者と前記決済サーバ間で利用者識別子と利用者秘密情報を取り決め、前記決済処理機能において、前記第2の決済要求に含まれる前記利用者識別子と前記利用者秘密情報とにより利用者の認証を行なうことを特徴とする請求項21乃至29いずれか一記載の決済サーバ。

【請求項31】 前記第2の決済要求に含まれる、決済処理に必要な利用者口座情報を用いて、前記決済処理機能を行なうことを特徴とする請求項21乃至30いずれか一記載の決済サーバ。

【請求項32】 決済処理に必要な利用者口座情報を予め保持しおき、前記利用者認証に成功した場合、保持した前記利用者口座情報を用いて前記決済処理機能により決済処理を行なうことを特徴とする請求項27、29又は30記載の決済サーバ。

【請求項33】 通信路で相互に接続された利用者端末、販売店サーバ、決済サーバとを備え、さらに前記決済サーバは、金融機関ホストマシンと接続され、

利用者が前記利用者端末と前記通信路を用いて、前記販売店サーバに物品もしくはサービスの注文要求を送る手段と、

前記販売店サーバが前記注文要求を受け付けると、前記決済サーバに第1の決済要求を送る手段と、

さらに前記利用者端末に支払処理要求を送る手段と、

前記利用者端末が前記支払処理要求を受け取り、第2の決済要求を前記決済サーバに送る手段と、

前記決済サーバが前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう決済処理手段と、

さらに、前記決済処理の結果を前記利用者端末に送る手段と、

前記利用者端末が前記決済処理結果を受け取ると、前記利用者端末から前記販売店サーバに決済処理結果を送る手段と、

前記販売店サーバが前記決済処理結果を受け取る手段と、を備えることを特徴とする電子決済システム。

【請求項34】 通信路で相互に接続された利用者端末、販売店サーバ、決済サーバとを備え、さらに前記決済サーバは、金融機関ホストマシンと接続され、

利用者が前記利用者端末と前記通信路を用いて、前記販売店サーバに物品もしくはサービスの注文要求を送る手段と、

前記販売店サーバが前記注文要求を受け付けると、前記決済サーバに第1の決済要求を送る手段と、

さらに前記利用者端末に支払処理要求を送信する手段と、

前記利用者端末が前記支払処理要求を受け取り、第2の決済要求を前記決済サーバに送る手段と、

前記決済サーバが前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう決済処理手段と、

さらに前記決済サーバが前記決済処理の結果を前記販売店サーバに送る手段と、

前記販売店サーバが前記決済処理結果を受け取る手段

と、

さらに前記決済サーバが前記決済処理の結果を前記利用者端末に送る手段と、

前記利用者端末が前記決済処理結果を受け取る手段と、を備えることを特徴とする電子決済システム。

【請求項35】 通信路で相互に接続された利用者端末、販売店サーバ、決済サーバとを備え、

さらに前記決済サーバは、金融機関ホストマシンと接続され、

10 利用者が前記利用者端末と前記通信路を用いて、前記販売店サーバに物品もしくはサービスの注文要求を送る手段と、

前記販売店サーバが前記注文要求を受け付けると、前記決済サーバに第1の決済要求を送る手段と、

さらに前記利用者端末に支払処理要求を送信する手段と、

前記利用者端末が前記支払処理要求を受け取り、第2の決済要求を前記決済サーバに送信する手段と、

20 前記決済サーバが前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう決済処理手段と、

さらに前記決済処理の結果を前記利用者端末に送る手段と、

前記利用者端末が前記決済処理結果を受け取る手段と、

前記販売店サーバは、前記決済処理の結果を前記決済サーバに問い合わせる手段と、

30 前記問い合わせを受けた前記決済サーバは、前記販売店サーバに前記決済処理の結果を返す手段と、

前記販売店サーバが前記決済処理の結果を受け取る手段と、を備えることを特徴とする電子決済システム。

【請求項36】 前記販売店サーバと前記決済サーバとで予め認証子の生成と検証を行なうための鍵を取り交わしておき、

前記決済サーバは、前記認証子生成用の鍵を用いて前記決済処理結果に対する認証子を生成し、前記利用者端末に送る前記決済処理結果に含ませ、

40 前記利用者端末は、前記決済処理結果を受け取り、前記販売店サーバに送る決済処理結果に前記認証子を含ませ、

前記販売店サーバは、前記決済処理結果を受け取り、前記決済処理結果に含まれる前記認証子と前記認証子検証用の鍵を用いて、前記決済処理結果の認証を行なうことを特徴とする請求項33記載の電子決済システム。

【請求項37】 前記販売店サーバと前記決済サーバの間の通信に、認証可能な通信方法を用い、

前記第1の決済要求の送受信において、前記認証可能な通信方法により、前記決済サーバと前記販売店サーバとの相互の認証を行なうことを特徴とする請求項33又は

36記載の電子決済システム。

【請求項38】 前記販売店サーバと前記決済サーバの間の通信に、認証可能な通信方法を用い、前記第1の決済要求の送受信および前記決済処理結果の送受信において、前記認証可能な通信方法により、前記決済サーバと前記販売店サーバとの相互の認証を行なうことを特徴とする請求項34又は35いずれか一記載の電子決済システム。

【請求項39】 前記利用者と前記決済サーバとで予め認証子の生成と検証を行なうための鍵と、前記利用者を識別する利用者識別子とを取り決めておき、前記利用者端末は、前記認証子生成用の鍵を用いて前記第2の決済要求に対する認証子を生成し、前記認証子と前記利用者識別子を前記第2の決済要求に含ませ、前記決済サーバは、前記決済処理手段において、前記第2の決済要求に含まれる前記利用者識別子から前記認証子検証用の鍵を特定し、前記認証子と前記認証子検証用の鍵により、前記利用者および前記第2の決済要求の認証を行なうことを特徴とする請求項33乃至38いずれか一記載の電子決済システム。

【請求項40】 前記利用者と前記決済サーバとで予め認証子の生成と検証を行なうための鍵を取り交わしておき、前記決済サーバは、前記認証子生成用の鍵を用いて前記決済処理の結果に対する認証子を生成し、前記決済処理の結果に含ませ、前記利用者端末は、前記決済処理結果を受け取る手段において、前記決済処理の結果に対する認証子と前記認証子検証用の鍵により、前記決済サーバと前記決済処理結果の認証を行なうことを特徴とする請求項33乃至39いずれか一記載の電子決済システム。

【請求項41】 前記利用者端末と前記決済サーバの間の通信に、認証可能な通信方法を用い、前記第2の決済要求と前記決済処理の結果の送受信において、前記認証可能な通信方法により、前記利用者と決済サーバとの相互の認証を行なうことを特徴とする請求項33乃至38いずれか一記載の電子決済システム。

【請求項42】 予め前記利用者と前記決済サーバ間で利用者識別子と利用者秘密情報を取り決め、前記第2の決済要求に、前記利用者識別子と前記利用者秘密情報を含み、前記決済サーバは、前記決済処理手段において、前記利用者識別子と前記利用者秘密情報により、利用者の認証を行なうことを特徴とする請求項33乃至38いずれか一記載の電子決済システム。

【請求項43】 決済処理に必要な利用者口座情報を前記第2の決済要求に含め、前記利用者口座情報を用いて前記決済サーバが決済処理を行なうことを特徴とする請求項33乃至42いずれか一記載の電子決済システム。

【請求項44】 決済処理に必要な利用者口座情報を前

記決済サーバで保持しておき、

前記決済サーバは、前記利用者認証が成功した場合に、保持した前記利用者口座情報により決済処理を行なうことを特徴とする請求項39、41又は42記載の電子決済システム。

【請求項45】 前記請求項16乃至19いずれか一の販売店サーバの処理内容を、情報処理装置を用いて実行させる販売店サーバプログラムを記録した記録媒体。

【請求項46】 前記請求項16乃至20いずれか一の販売店サーバの処理内容を、情報処理装置を用いて実行させる販売店サーバプログラムを通信路を介して伝送する伝送媒体。

【請求項47】 前記請求項21乃至32いずれか一の決済サーバの処理内容を、情報処理装置を用いて実行させる決済サーバプログラムを記録した記録媒体。

【請求項48】 前記請求項21乃至請求項32いずれか一の決済サーバの処理内容を、情報処理装置を用いて実行させる決済サーバプログラムを伝送する伝送媒体。

【請求項49】 利用者端末と、この利用者端末と通信路を介して接続された販売店サーバと、前記利用者端末及び前記販売店サーバと通信路を介して接続された決済サーバとを使用して電子決済を行うための電子決済用プログラムを記憶した記憶媒体であって、前記電子決済用プログラムは前記決済サーバを動作させる指令として、

前記利用者端末の保持者である利用者から前記販売店へ注文があったときに当該注文の決済要求を第1の決済要求として受信させる第1の受信指令と、

前記注文の決済要求を前記利用者端末から受信させる第2の受信指令と、

前記第1の決済要求と前記第2の決済要求との受信に応じて前記第1の決済要求の内容と前記第2の決済要求の内容とを照合させる決済要求照合指令と、

この決済要求照合指令に応じて前記第1及び第2の決済要求の内容に不整合がない場合に当該決済処理を実行させる決済処理指令とを備えたことを特徴とする電子決済用プログラムを記憶した記憶媒体。

【請求項50】 利用者端末と、この利用者端末と通信路を介して接続された販売店サーバと、前記利用者端末及び前記販売店サーバと通信路を介して接続された決済サーバとを使用して電子決済を行うための電子決済用プログラムを記憶した記憶媒体であって、前記電子決済用プログラムは前記販売店サーバを動作させる指令として、

前記利用者端末の利用者から注文を受けたときに当該注文内容と当該注文及び利用者を識別する識別番号と共に前記決済サーバに第1の決済要求として送信させる指令と、

前記注文内容を前記利用者端末へ支払処理要求として送信させる指令と、

前記決済サーバ又は前記利用者端末から前記注文及び利用者を識別する識別番号と共に前記決済の結果を受信させる指令とを備えたことを特徴とする電子決済用プログラムを記憶した記憶媒体。

【請求項51】 利用者端末と、この利用者端末と通信路を介して接続された販売店サーバと、前記利用者端末及び前記販売店サーバと通信路を介して接続された決済サーバとを使用して電子決済を行うための電子決済用プログラムを記憶した記憶媒体であって、
前記電子決済用プログラムは、前記利用者端末を動作させる指令として、

当該利用者端末の利用者から注文を受けた前記販売店サーバから当該注文内容と当該注文及び利用者を識別する識別番号とを支払要求指令として受信させる支払要求指令受信指令と、

この支払要求指令受信指令の受信に応じて当該支払要求の決済を前記決済サーバに要求するための第2の決済要求を前記注文及び利用者の識別番号と共に前記決済サーバに送信させる第2の決済要求送信指令と、

この第2の決済要求送信指令に応じて動作する決済サーバから当該注文内容の決済結果を受信させる決済結果受信指令とを備えたことを特徴とする電子決済用プログラムを記憶した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、利用者から注文を受けた物品またはサービスに対する代金の決済を、ネットワークを介して行なう電子決済方法および電子決済システムに関する。

【0002】

【従来の技術】インターネット等のネットワークを用いて、利用者から注文を受けた物品またはサービスに対する代金の決済を行なう従来の電子決済システムのブロック図を図14に示す。買手である利用者は、利用者端末42と通信路45を用いて、売手の販売店サーバ41に注文要求を送る。これを受けた販売店サーバ41は、利用者端末42に利用者のクレジットカード番号や銀行口座番号などの利用者口座情報の要求を送信する。利用者は利用者端末42を用いて、上記の利用者口座情報を販売店サーバ41に送る。

【0003】販売店サーバ41は、上記の利用者口座情報に基づく決済要求を、通信路44を通じて決済サーバ43に送出する。決済サーバ43は、この決済要求を金融機関ホストマシンとの連携により処理し、その決済処理結果を販売店サーバ41に返す。販売店サーバ41では、上記の決済処理結果を、通信路45を通じて利用者端末42に返す。

【0004】この図14に示す構成により、現金を用いずに商品やサービスの購入の決済を行うことができる。

【0005】

【発明が解決しようとする課題】しかしながら、上記従来例による情報の流れで決済を行なった場合、売手側の販売店サーバに利用者のクレジットカード番号や銀行口座番号などの利用者口座情報が露呈し、売手側に悪用される危険性がある、という不都合があった。また、決済金額が売手側のみから金融機関に行くので、金額を改ざんされる危険性もある。

【0006】これを防止するために、SETやSECEなどのプロトコルがある。これらのプロトコルでは、利用者口座情報の暗号化や、決済金額への電子署名付与などが行われ、前述の危険性を回避することが可能である。しかし、暗号化や電子署名の生成を行なうためには、利用者側に暗号化や署名生成のためのプログラムと電子証明書を用意する必要があり、それを用意するために利用者に作業の負担や費用的な負担を強いることになる。

【0007】

【発明の目的】そこで、本発明の目的は、暗号化や署名生成のためのプログラムと電子証明書を用意する利用者側の負担及びハードウェア資源の負担とを軽減し、なおかつ、売手側に利用者のクレジットカード番号や銀行口座番号などの利用者口座情報を秘匿でき、利用者が安全性に関して判りやすい電子決済方法を提供することにある。

【0008】

【課題を解決するための手段】そこで、本発明では、利用者端末と通信路を介して接続された販売店サーバと、前記利用者端末及び前記販売店サーバと通信路を介して接続された決済サーバとを使用して電子決済を行う電子決済方法であって、販売店サーバが、前記利用者端末から送信される物品若しくはサービスの注文要求を受信するステップと、販売店サーバが、前記注文要求に関する決済処理の依頼を前記決済サーバに第1の決済要求として送信するステップとを備えている。続いて、決済サーバが、前記第1の決済要求の受信と前後して、前記利用者端末から前記注文要求を行った注文に関する決済処理の依頼を第2の決済要求として受信するステップと、決済サーバが、前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に決済処理を行う決済処理ステップとを備えた、という構成を採っている。これにより前述した目的を達成しようとするものである。

【0009】本発明では、利用者と販売店で商取引の申込がなされると、販売店サーバと利用者サーバの双方から決済サーバへ決済要求を行う。すなわち、決済サーバは、第1の決済要求を販売店サーバから受信し、第2の決済要求を利用者端末から受信する。決済サーバは、第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを

照合し、不整合がない場合に決済処理を行う（決済処理ステップ）。このため、販売店と利用者双方の決済要求が一致していない場合には、決済処理は不成立となる。また、決済に必要な利用者の個人情報、利用者端末からのみ送信されても注文内容及び金額の比較で決済を行うことができるため、利用者の個人情報が販売店へ漏洩することがない。

【0010】好ましい実施形態では、決済結果の伝達に関して種々の構成を採り得る。第1の電子決済方法では、販売店サーバと利用者端末の双方から決済サーバに決済要求を出し、利用者口座情報は利用者端末からの決済要求にのみ含める。決済サーバによる決済処理結果は、利用者端末を経由して販売店サーバに返される。より具体的には、利用者は利用者端末を用いて販売店サーバに注文要求を出し、これを受けて販売店サーバは決済サーバと利用者端末の双方に決済要求を出す。利用者は利用者端末を用いて決済要求を受け、自分のクレジットカード番号や銀行口座番号などの利用者口座情報を含めた決済要求を決済サーバに送る。決済サーバは双方からの要求内容に相違がないか確認後に決済処理を行ない、決済処理結果を利用者端末に返し、利用者端末は販売店サーバに決済処理結果を返す。

【0011】また、第2の電子決済方法および電子決済システムは、第1の電子決済方法と同様に、販売店サーバと利用者端末の双方から決済サーバに決済要求を出し、利用者口座情報は利用者端末からの決済要求にのみ含める。第1の電子決済方法と異なる点は、決済サーバによる決済処理結果を、決済サーバから利用者端末と販売店サーバの双方に直接、返す点である。

【0012】また、第3の電子決済方法および電子決済システムは、第1の電子決済方法と同様に、販売店サーバと利用者端末の双方から決済サーバに決済要求を出し、利用者口座情報は利用者端末からの決済要求にのみ含める。第1の電子決済方法と異なる点は、決済サーバによる決済処理結果は、決済サーバから利用者端末に返され、販売店サーバは別途、決済サーバに決済処理結果を問い合わせ、その問い合わせを受けた決済サーバは決済処理結果を販売店サーバに通知する点である。

【0013】

【発明の実施の形態】次に本発明の電子決済方法および電子決済システムの実施の形態について図面を参照して詳細に説明する。

【0014】＜第1実施形態＞図1を参照すると、本発明の電子決済方法の第1の実施の形態は、販売店サーバ11と、利用者端末12と、決済サーバ13と、決済サーバ13と販売店サーバ11を結ぶ通信路14と、販売店サーバ11と利用者端末12を結ぶ通信路15と、利用者端末12と決済サーバ13を結ぶ通信路16と、決済サーバ13に接続された金融機関ホストマシン17とから構成されている。

【0015】通信路14と通信路15と通信路16は、インターネット等の汎用的なネットワークであってもいいし、専用の通信回線などであってもいい。通信路14と通信路15と通信路16が異なる通信路であっても構わないし、すべてインターネット等の同一の通信路であっても構わない。また、それぞれは移動通信網とインターネット等による複合的な通信網としても良い。

【0016】販売店サーバ11は、製品やサービスの販売者、もしくはその代行者により使用され、ワークステーション・サーバ等の情報処理装置によって構成される。販売店サーバ11は、単一の販売店向けのサーバであってもよく、複数の販売店向けの共同サーバであってもよい。販売店サーバ11は、通信路15を介して、利用者端末からの注文要求を受け付ける機能を備えている。また、注文要求を受け付けた際、通信路14を介して決済サーバに第1の決済要求を送る機能と、通信路15を介して支払処理要求を利用者端末に送る機能を備えている。さらに、通信路15を介して利用者端末から決済処理結果を受け取る機能を備えている。販売店サーバ11は、単一の情報処理装置から構成されてもよいが、注文要求を受け付ける機能と、決済要求と結果取得を行なう機能とを別々の情報処理装置で行なう等、複数の情報処理装置から構成することも可能である。

【0017】ここでいう決済要求とは、物品やサービスに対する代金の承認確認（クレジット決済の場合の与信確認や銀行決済の残高確認）や代金回収を指す。また、広く承認取消や返金なども含めて考えることもできる。

【0018】利用者端末12は、パーソナルコンピュータや携帯端末、情報家電などの情報処理装置である。利用者端末12に必要な機能は、第1に販売店サーバ11および決済サーバ13と注文要求や決済要求、決済処理結果の送受信を行なう通信機能、第2に販売店サーバ11からの決済要求の内容や決済サーバ13からの決済処理結果を利用者の確認のために表示する決済結果表示機能、第3に注文内容やクレジットカード番号や銀行口座番号などの利用者口座情報を入力するための入力機能である。通信網15および通信網15がインターネットであれば、これらの機能はパーソナルコンピュータとブラウザソフトで実現でき、多くの携帯端末や情報家電では標準で備えている機能である。

【0019】利用者端末12が、パーソナルコンピュータ、携帯端末、情報家電の場合には、それぞれの機器を用いて注文を行うことができる。すなわち、利用者端末12を操作することで注文を販売店サーバに送信できる。また、携帯端末を用いると、実際の店舗での物品の購入やサービスの提供等に対する支払に用いることもできる。この場合、利用者は携帯端末の番号等を販売店に知らせるか、携帯端末とデータの送受信が可能な機器を店舗のレジ等に設けておくことで実現できる。販売店サーバは支払処理要求を当該利用者端末へ送信する。

【0020】決済サーバ13は、クレジットカード会社や銀行などの決済事業者、もしくはその代行者により使用され、ワークステーション・サーバ等の情報処理装置によって構成される。決済サーバは、通信路14を介して販売店サーバ11から第1の決済要求を受け取る機能、および、通信路15を介して利用者端末12から第2の決済要求を受け取る機能を備えている。決済に必要なクレジットカード番号や銀行口座番号など、利用者個人の利用者口座情報は、利用者端末12からの第2の決済要求で受け取る。両者からの決済要求には、注文を特定する同一の識別情報を含むものとし、決済サーバ13はこの識別情報により両者からの決済要求を同一の注文に対するものと認識する。

【0021】さらに、決済サーバ13は、第1の決済要求および第2の決済要求に基づき、決済処理を行なう。これは金融ネットワーク等を介して別途、接続された金融機関ホストマシン17と決済処理に関する情報をやり取りすることにより行われる。また、決済サーバ13は、決済処理の結果を通信路16を介して接続された利用者端末12に送信する機能を備えている。決済サーバ13は、単一の情報処理装置から構成されてもよいが、販売店サーバ11との通信部分と、利用者端末12との通信部分と、金融機関ホストマシンとの通信処理部分とを別々の情報処理装置で行なう等、複数の情報処理装置から構成することも可能である。

【0022】次に、本発明の第1実施形態での代表的な動作例を図2乃至図6を参照して説明する。ここでは、通信路15および通信路16はインターネットであるとし、利用者端末12はインターネットのブラウザ機能を有する端末機器とする。図2及び図3は、符号Aa、Ab、Acにて処理が連続している。

【0023】まず、販売店サーバ11には、インターネット（通信路15）を介して利用者端末12からの注文要求を受け付けるため、販売店サーバ11に図4に例示するような画面を用意しておく。買手である利用者は、利用者端末11を用い、インターネット（通信路15）を介して販売店サーバ11に接続し、図4に例示するような画面を表示し、注文したい商品の名前、商品コード、個数を選択または入力する。さらに届け先、名前、連絡先などの情報を入力する。必要事項を入力し、図4に示すような画面の注文実行ボタンを操作することで、利用者は注文要求を販売店サーバ11に送る（図2ステップA1）。これはHTTPプロトコルのPOSTなどのメソッドで実現できる。ここでいう注文要求には、利用者が入力した商品の名前や商品コード、個数、届け先、名前、連絡先などの情報を含むものとする。

【0024】販売店サーバ11は、CGIスクリプトなどで上記の注文要求を受信する（ステップA2）。ここで販売店サーバは、注文を特定するための識別番号を割り当てる。また必要であれば、在庫の確保などの商品管

理に必要な処理や、商品発送に必要な処理を行なう。

【0025】次いで、販売店サーバ11は、通信路14を介して、決済サーバ13に第1の決済要求を送る（ステップA3）。第1の決済要求は、注文を特定するための前述の識別番号を含む。また、注文内容として、商品名や単価、個数などの情報を含める。またこれは注文内容のHash値（一方方向関数で圧縮した値）でも構わない。通信路14がインターネットであれば、この第1の決済要求の送信は、HTTPプロトコルのPOSTなどのメソッドで実現できる。

【0026】決済サーバ13は、上記の第1の決済要求を受け付ける（ステップA4）。これは通信路14がインターネットであれば、CGIスクリプトなどで実現できる。第1の決済要求を受け付けた決済サーバ13は、内部にこの要求を保持する。必要であれば、第1の決済要求を受け付けた決済サーバ13は、要求受付の応答（レスポンス）を販売店サーバ11に返し（ステップA5）、販売店サーバ11はこれを受け付ける（ステップA6）。

【0027】ここまでの説明では、注文を特定する識別番号を販売店サーバが割り当てていたが、決済サーバ13が第1の決済要求を受け付けた時点で決済サーバ13が注文を特定する識別番号を割り当て、要求受付の応答として販売店サーバに通知する方法でも構わない。

【0028】次いで、販売店サーバ11は、利用者端末12に、支払処理要求を送信する（ステップA7）。これは、HTTPプロトコルのPOSTなどのメソッドで送られた注文要求のレスポンスとして送ることで実現できる。この支払処理要求には、注文を特定するための前述の識別番号、および注文内容として商品名や単価、個数などの情報を含める。

【0029】利用者端末12は、注文要求のレスポンスとして支払処理要求を販売店サーバ11から受け取り（ステップA8）、これを決済サーバ13に転送する（ステップA9）。これはHTTPプロトコルのリダイレクトの機能を用いても実現できるし、もしくは、支払処理要求として画面を返し、その画面上のボタンを利用者にクリックさせることで支払処理要求を決済サーバ13に転送させることでも実現できる。

【0030】決済サーバ13は、転送された支払処理要求を受け付け（ステップA10）、これを基に第2の決済要求の表示・入力画面を利用者端末13に返す（ステップA11）。この第2の決済要求の表示・入力画面を図5に例示する。この画面には、注文した商品名、商品コード、単価、個数、合計金額などを表示することができる。また、注文を特定する識別番号も含む。さらに、利用者口座情報の記入欄、決済実行ボタンを含む。図5ではクレジットカード決済時の例として、クレジットカード番号の入力欄を例示しているが、銀行決済の場合は口座番号と暗証番号などの入力欄になる。

【0031】利用者端末12は、第2の決済要求の表示・入力画面を、決済サーバ13から受け取り（図3のステップA12）、これを表示する（ステップA13）。

【0032】なお、上記のステップA9からステップA13の説明では、支払処理要求を決済サーバ13に転送し、決済サーバ13で第2の決済要求の表示・入力画面を用意する実施方法を説明したが、販売店サーバ11がステップA7で支払処理要求を第2の決済要求の表示・入力画面として利用者端末12に送る方法もある。また、販売店サーバ11がステップA7で利用者端末12側の専用ソフトウェアを起動し、その専用ソフトウェアが第2の決済要求の表示・入力画面を用意する方法もある。これらの場合、ステップA9からステップA12は不要となる。

【0033】利用者は、この第2の決済要求の表示・入力画面で注文内容を確認し、間違いがなければ、利用者口座情報として、クレジットカード番号や、口座番号と暗証番号などの記入欄に必要事項を記入する（ステップA14）。

【0034】利用者が利用者口座情報を入力し、決済実行ボタンをクリックすると、第2の決済要求が、通信路16を介して、決済サーバ13に送られる（ステップA15）。これはHTTPプロトコルのPOSTなどのメソッドで実現できる。ここでいう第2の決済要求には、利用者が注文した商品の名前や商品コード、個数、注文を特定する識別番号、および、利用者が入力したクレジットカード番号や、口座番号と暗証番号などの利用者口座情報を含む。

【0035】決済サーバ13は、CGIスクリプトなどで上記の第2の決済要求を受信する（ステップA16）。

【0036】第2の決済要求を受信した決済サーバ13は、要求の内容を先に受けた第1の決済要求と照合する（ステップA17）。注文が同時に複数ある場合、決済サーバ13は複数の第1の決済要求を保持していることになるが、注文を特定する識別番号により、対応する第1の決済要求を特定することは可能である。照合の処理は、第1の決済要求と第2の決済要求で商品の種類や個数、金額等に相違がないかを照合する。これにより、販売店もしくは利用者が注文内容を改ざんし、不正な注文もしくは決済を行なうことを防止できる。

【0037】上記の照合により異常等の不整合が検出されなかった場合、決済サーバ13は、決済処理を行なう（ステップA18）。これは、第1の決済要求に含まれる、利用者のクレジットカード番号や口座番号などの利用者口座情報に基づき、決済処理を行なうものであり、金融ネットワーク等を介して別途、接続された金融機関ホストマシン17と決済処理に関する情報をやり取りすることにより実現できる。代金を受け取る売手側の口座情報（銀行口座番号など）は、第1の決済要求で販売店

サーバ11から受け取ってもいいし、決済サーバ13で予め保持していてもいい。

【0038】決済処理が終わると、決済サーバ13は決済処理結果を利用者端末12に送信する（ステップA19）。これは、HTTPプロトコルのPOSTなどのメソッドで送られた第2の決済要求のレスポンスとして、HTML画面を返すことで実現できる。

【0039】利用者端末12は、この決済処理結果画面を受信し（ステップA20）、表示する（ステップA21）。この画面の例を図6に示す。利用者はここで決済処理の結果を確認し、さらに、画面の指示に従い、利用者が決済処理結果を販売店サーバに送るボタンをクリックすると、販売店サーバに決済処理結果を送信する（ステップA22）。これはHTTPプロトコルのPOSTなどのメソッドで実現できる。販売店サーバ11は利用者端末12から送られた決済処理結果を受信し（ステップA23）、商品発送などの必要な処理を行なう。

【0040】なお、上記の説明では、利用者は決済サーバ13からステップA19で返された図6で例示した画面で決済処理結果を確認し、利用者のボタン操作により販売店サーバ11に決済処理結果が返る実施例で説明しているが、他の実施方法としては、決済サーバ13からの利用者端末12に返された決済処理結果を直接、HTTPプロトコルのリダイレクトの機能により販売店サーバ11に転送し、利用者は販売店サーバ11からのレスポンスの画面で決済処理結果を確認する方法もある。

【0041】上記の第1の実施の形態では、利用者端末12を経由して決済処理結果が販売店サーバ11に返される。従って、悪意のある利用者が決済処理結果を偽造し、不正を行なう可能性もあるが、それは以下の方法などで検知できる。

【0042】まず、販売店サーバ11と決済サーバ13とで予め認証子の生成と検証を行なうための鍵を取り交わしておく。ここでいう認証子とは、秘密鍵暗号（対称鍵暗号）を用いたMACや、公開鍵暗号を用いたデジタル署名などを指す。

【0043】決済サーバ13は、上記の認証子生成用の鍵を用いて決済処理結果に対する認証子を生成し、利用者端末12に送る前記決済処理結果に含ませる。利用者端末13は、決済サーバ13からの決済処理結果を受け取り、販売店サーバ11に送る決済処理結果に前記の認証子を含ませる。販売店サーバ11は、前記の決済処理結果を受け取り、そこに含まれる認証子と予め取り交わした認証子検証用の鍵を用いて、決済処理結果の認証を行なう。利用者は、販売店サーバ11と決済サーバ13との間で鍵を取り交わされた鍵を知り得ない限り、認証子を偽造することは不可能であり、決済処理結果の偽造は検知できる。

【0044】次に、図1を再度参照して再度電子決済システムの構成を説明する。図1に示す電子決済システム

は、各端末やサーバが備える機能の点からは、次の構成を採る。すなわち、電子決済システムは、通信路14、15、16で相互に接続された利用者端末12、販売店サーバ11、決済サーバ13とを備えている。そして、決済サーバ13は、金融機関ホストマシン17と接続されている。

【0045】利用者端末は、利用者の操作に応じて、通信路15を用いて、前記販売店サーバ11に物品もしくはサービスの注文要求を送る手段12Aと、販売店サーバ11からの支払処理要求を受け取り、第2の決済要求を決済サーバ13に送る手段12Bとを備えている。

【0046】販売店サーバ11は、注文要求を受け付けたときに決済サーバ13に第1の決済要求を送る手段11Aと、利用者端末に支払処理要求を送る手段11Bとを備えている。

【0047】前記決済サーバは、前記第1の決済要求と前記第2の決済要求を受け取ると、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に前記金融機関ホストマシンとにより決済処理を行なう決済処理手段13Aを備えている。

【0048】そして、第1実施形態では、決済サーバが、前記決済処理の結果を前記利用者端末12に送る手段13Bを備え、利用者端末12が、前記決済処理結果を受け取ったときに利用者端末12から前記販売店サーバに決済処理結果を送る手段12Cを備え、販売店サーバ11が、前記決済処理結果を受け取る手段11Cを備えている。この構成により、図2及び図3に示した処理が行われる。

【0049】＜第2実施形態＞次に、本発明の第2の実施の形態について図面を参照して詳細に説明する。本発明の第2の実施の形態は、販売店サーバ21へ決済処理結果を返す方法が、決済サーバ23から利用者端末22を介して販売店サーバ21に返すのではなく、直接、決済サーバ23から販売店サーバ21に返す点で第1の実施の形態と異なる。

【0050】図7は、第2実施形態の構成例を示すブロック図である。第2の実施の形態における販売店サーバ21、利用者端末22、決済サーバ23、通信路24乃至通信路26、金融機関ホストマシン27の構成、および個々の必要機能は、第1の実施の形態と次の点を除いて同じである。それは、決済サーバ23が販売店サーバ21に通信路24を介して決済処理結果を送る機能と、販売店サーバ21が通信路24を介して決済サーバ23から決済処理結果を受け取る機能を有することである。

【0051】次に、図8及び図9を参照して、第2の実施の形態の動作について説明する。図8及び図9に示す例では、符号Ba、Bb、Bcにてそれぞれ処理が連続している。ここでも通信路25および通信路26はインターネットであるとし、利用者端末22はインターネットのブラウザ機能を有する端末機器とする。決済サーバ

が決済処理を行なうまでの図8及び図9のステップB1からステップB18までは、第1の実施の形態のステップA1からステップB18までと同じである。

【0052】決済処理（ステップB18）が終わると、決済サーバ23は、まず、決済処理結果を、販売店サーバ21に返す（ステップB19）。これは、HTTPプロトコルのPOSTなどのメソッドを用いれば実現できる。もしくは、決済サーバ23が販売店サーバ21に電子メールを出すことによって実現できる。

【0053】販売店サーバ21は、上記の決済処理結果を受け取り（ステップB20）、必要に応じ、決済が認められれば注文に対する商品発送などの処理を行ない、決済が認められなければ決済の中止や再要求などの処理を行なう。これは販売店サーバ21でのCGIスクリプト等により実現できる。

【0054】上記ステップ19においてHTTPプロトコルのPOSTなどのメソッドを持ちいた場合、決済処理結果を受け取った販売店サーバ11は、レスポンスとして受信できた旨を決済サーバ23に送り（ステップB21）、決済サーバ23はこれを受け取る（ステップB22）。ただし、ステップ19において電子メールを用いた場合にはステップB21およびステップB22は不要である。

【0055】次いで決済サーバ23は、決済処理結果を、利用者端末22に送信する（ステップB23）。これは、HTTPプロトコルのPOSTなどのメソッドで送られた第2の決済要求のレスポンスとして、HTML画面を返すことで実現できる。利用者端末22がこの画面を受信し（ステップB24）、表示する（ステップB25）。

【0056】この第2実施形態では、図1に示す構成と比較して、決済サーバが前記決済処理の結果を前記販売店サーバに送る手段23Cを備え、販売店サーバが前記決済処理結果を受け取る手段21Dを備える点で相違する。また、図1の符号11C及び12Cで示す手段は備えていない。

【0057】＜第3実施形態＞次に、本発明の第3の実施の形態について図面を参照して詳細に説明する。本発明の第3の実施の形態は、販売店サーバ31へ決済処理結果を返す方法が、決済サーバ33から利用者端末32を介して販売店サーバ31に返すのではなく、販売店サーバ31が決済サーバ33に決済処理結果を問い合わせ、これを受けた決済サーバ33が販売店サーバ31に決済処理結果を返す点で第1の実施の形態と異なる。

【0058】図10は、本発明の第3実施形態の構成例を示すブロック図である。第3の実施の形態における販売店サーバ31、利用者端末32、決済サーバ33、通信路34乃至通信路36、金融機関ホストマシン27の構成、および個々の必要機能は、第1の実施の形態と次の点を除いて同じである。それは、販売店サーバ31が

決済サーバ33に通信路34を介して決済処理結果の問い合わせ要求を送る機能と、決済サーバ33が決済処理結果を保持し、販売店サーバ31からの問い合わせ要求を受け付けて、要求された決済処理結果を販売店サーバ31に返送する機能を有することである。

【0059】次に、図11及び図12を参照して、第3の実施の形態の動作について説明する。図11及び図12に示す例では、符号Ca、Cb、Ccにてそれぞれ処理が連続している。ここでも通信路35および通信路36はインターネットであるとし、利用者端末32はインターネットのブラウザ機能を有する端末機器とする。

【0060】決済サーバが決済処理を行なうまでの図11及び図12のステップC1からステップC18までは、第1の実施の形態のステップA1からステップC18までと同じである。

【0061】決済処理（ステップC18）が終わると、決済サーバ23は、決済処理結果を、利用者端末32に送信する（ステップC19）。これは、HTTPプロトコルのPOSTなどのメソッドで送られた第2の決済要求のレスポンスとして、HTML画面を返すことで実現できる。利用者端末32がこの画面を受信し（ステップC20）、表示する（ステップC21）。なお、決済サーバ33は決済処理結果を一定期間、履歴として保持するものとする。

【0062】一方、販売店サーバ31は、決済処理結果を決済サーバ33に問い合わせる（ステップC22）。これは、決済要求を行なってから一定時間経過後や、注文を受けた日や翌日の定刻などに行なえばよい。HTTPプロトコルのPOSTなどのメソッドを用いれば実現できる。

【0063】決済サーバ33は、販売店サーバ31からの問い合わせを受信する（ステップC23）。これはCGIスクリプトなどで実現できる。そして、保持している履歴を検索し、問い合わせられた決済要求の結果を検索する（ステップC24）。この検索は、第1の決済要求に含まれる注文を特定する識別番号を決済処理結果と共に履歴として保持し、販売店サーバ11からの問い合わせ要求にその識別番号を含ませ、その識別番号をキーに履歴を検索すればよい。

【0064】決済サーバ33は、検索された決済処理結果を販売店サーバ31に返信する（ステップC25）。販売店サーバ31は、決済サーバ33からの応答として決済処理結果を受け取り（ステップC25）、必要に応じて、決済が認められれば注文に対する商品発送などの処理を行ない、決済が認められなければ決済の中止や再要求などの処理を行なう。

【0065】再度図10を参照すると、第3実施形態では、図1に示す構成と異なり、販売店サーバ31が、前記決済処理の結果を前記決済サーバに問い合わせる手段31Eを備えている。そして、決済サーバ33は、販売

店サーバに前記決済処理の結果を返す手段33Dを備えている。また、販売店サーバ31は、前記決済処理の結果を受け取る手段31Fを備えている。

【0066】＜各実施形態の共通事項＞図13は、販売店サーバ11、21、31や、決済サーバ13、23、33や、利用者端末12、22、32として動作する情報処理装置50A、50B、50Cの一般的構成例を示すブロック図である。図1に示す例では、情報処理装置は、オペレーティングシステムを構成するプログラムや、他のプログラムを実行するCPU51と、このCPU51の主記憶となるRAM52と、オペレーティングシステム用のプログラムや、他のプログラムや、各プログラムが使用するデータ等を記憶したハードディスク（補助記憶装置）53と、CD-ROM等の記憶媒体54Aを駆動するディスクドライブとを備えている。CPUは、ディスクドライブ54によって読み出されるプログラムを、ハードディスク等に格納し、利用者の操作に応じてプログラムデータを読み出し、実行する。情報処理装置50Aは、キーボード等の入力部55と、ディスプレイ等の表示部56とを備えている。

【0067】情報処理装置50Aが、決済サーバを駆動するための電子決済用プログラムを実行すると、図1等に示す決済サーバとして機能する。同様に、販売サーバを駆動するための電子決済用プログラムを情報処理装置Bが実行すると、情報処理装置Bは販売サーバとして機能する。利用者端末についても同様である。

【0068】この決済サーバを動作させる電子決済用プログラムは、利用者端末の保持者である利用者から前記販売店へ注文があったときに当該注文の決済要求を第1の決済要求として受信させる第1の受信指令（ステップA5に対応）と、注文の決済要求を前記利用者端末から受信させる第2の受信指令（ステップA16に対応）と、第1の決済要求と前記第2の決済要求との受信に応じて前記第1の決済要求の内容と前記第2の決済要求の内容とを照合させる決済要求照合指令（ステップA17に対応）と、この決済要求照合指令に応じて前記第1及び第2の決済要求の内容に不整合がない場合に当該決済処理を実行させる決済処理指令（ステップA18に対応）とを備えている。

【0069】情報処理装置50Aが、この決済サーバ向けの電子決済用プログラムを実行すると、図1等に示す決済サーバとして機能し、また、図2及び図3等に示す処理を実行する。

【0070】販売店サーバを動作させる電子決済用プログラムは、利用者端末の利用者から注文を受けたときに当該注文内容と当該注文及び利用者を識別する識別番号と共に前記決済サーバに第1の決済要求として送信させる指令（ステップA3に対応）と、注文内容を前記利用者端末へ支払処理要求として送信させる指令（ステップA7に対応）と、決済サーバ又は前記利用者端末から前

記注文及び利用者を識別する識別番号と共に前記決済の結果を受信させる指令（ステップA23、B20、C26等に対応）とを備えている。

【0071】また、情報処理装置50Cが、利用者端末を動作させるための電子決済用プログラムを実行すると、この情報処理装置50Cは利用者端末として機能する。この利用者端末を動作させるための電子決済用プログラムは、利用者端末の利用者から注文を受けた前記販売店サーバから当該注文内容と当該注文及び利用者を識別する識別番号とを支払要求指令として受信させる支払要求指令受信指令（ステップA8に対応）と、この支払要求指令受信指令の受信に応じて当該支払要求の決済を前記決済サーバに要求するための第2の決済要求を前記注文及び利用者の識別番号と共に前記決済サーバに送信させる第2の決済要求送信指令（ステップA15に対応）と、この第2の決済要求送信指令に応じて動作する決済サーバから当該注文内容の決済結果を受信させる決済結果受信指令（ステップA20に対応）とを備えている。

【0072】各プログラムをそれぞれの情報処理装置へ導入するには、種々の手法を取り得る。図13に示す例では、記憶媒体54Aに決済サーバ用のプログラムを格納しておき、ディスクドライブ54を介して情報処理装置に導入するようにしても良い。また、プログラムのダウンロードが可能なWebサイト（WWWサーバ）によって管理されるハードディスク等の記憶媒体からダウンロードしても良い。また、cgi等のスクリプトを用いて動的にhtmlページを生成する場合には、決済サーバから利用者端末へ向けて利用者端末用の電子決済用プログラムを逐次送信するようにしても良い。

【0073】第1の実施形態において、販売店サーバ11と決済サーバ13の間の通信に、前述のような認証可能な通信方法を用いることで、決済サーバ13が販売店サーバ11の認証を行なうことが可能である。つまり、第1の決済要求の送受信において、認証可能な通信方法を用いることにより、決済サーバ13は正規の販売店サーバ11から送られた正規の決済要求であることを確認でき、販売店サーバ11は正規の決済サーバ13に決済要求を送ったことを確認できる。ここでいう認証可能な通信方法とは、専用線を用いて通信を行なう方法や、電子証明書を用いたSSL通信を行なうなどである。

【0074】これは第2の実施形態においても同じであるが、第2の実施形態ではさらに、販売店サーバ21と決済サーバ23の間の通信で認証可能な通信方法を用いることで、決済処理結果の送受信において販売店サーバ21と決済サーバ23との相互の認証が可能である。つまり、販売店サーバ21は正規の決済サーバ23から返された正規の決済処理結果であることを確認でき、決済サーバ23は正規の販売店サーバ21に決済処理結果を送ったことを確認できる。

【0075】またこれは第3の実施形態においても第2の実施形態と同じで、第3の実施形態ではさらに、決済サーバ33は正規の販売店サーバ31からの決済処理結果の問い合わせ要求を受けたことを確認できる。

【0076】第1の実施形態において、決済サーバにおける利用者認証、および利用者端末における決済サーバ認証は、以下のような方法で行なうことができる。1つの方法は、まず、利用者（決済サーバ13）とで予め認証子の生成と検証を行なうための鍵と、利用者を識別する利用者識別子とを取り決めておく。ここでいう認証子とは、秘密鍵暗号（対称鍵暗号）を用いたMACや、公開鍵暗号を用いたデジタル署名など指す。

【0077】利用者端末12は、第2の決済要求の決済要求を決済サーバ13に送る際、前記の認証子生成用の鍵を用いて第2の決済要求に対する認証子を生成し、この認証子と前記の利用者識別子を第2の決済要求に含ませる。

【0078】決済サーバ13は、決済処理（ステップA18）において、第2の決済要求に含まれる利用者識別子から認証子検証用の鍵を特定し、この鍵と前記の第2の決済要求に対する認証子により利用者および決済要求の認証を行なう。これにより、正規の利用者による正規の決済要求であることを決済サーバ13は検証できる。逆に、決済サーバ13は、利用者端末12に返す決済処理結果に、決済処理結果に対する認証子を含ませる。利用者端末12は、決済処理結果の受信処理において、前記の決済処理結果に対する認証子により、決済サーバ13および決済処理結果の認証を行なう。これにより、正規の決済サーバ13による正規の決済処理結果であることを利用者端末12は検証できる。

【0079】上記の認証子を用いる方法では、予め利用者端末12と決済サーバ13との間で、認証子の生成、検証に用いる鍵を取り替えしておく必要がある。また、認証子の生成においては、専用のソフトウェアが必要になる場合があるが、そのソフトウェアは予め決済サーバ13からダウンロードし、利用者端末12にインストールできるようにしておけばいい。このソフトウェアは、SETにおけるワレットソフトと同様に販売店サーバ11からの支払処理要求で起動し、認証子を生成して決済して第2の決済要求を決済サーバ13に送り、決済サーバ13からの決済処理結果を受信し、そこに含まれる決済要求の結果の認証子を検証すればよい。

【0080】決済サーバと利用者間の相互認証を行なう別の方法としては、利用者端末12と決済サーバ13の間の通信に、前述のような認証可能な通信方法を用いる方法もある。つまり、第2の決済要求と決済処理結果の送受信において、認証可能な通信方法により、利用者端末12と決済サーバ13との相互の認証を行なえばよい。

【0081】決済サーバにおける利用者認証は、IDと

パスワードを用いることによっても実現できる。つまりこれは、予め利用者と決済サーバ間で利用者識別子なるIDと、利用者秘密情報であるパスワードを取り決め、第2の決済要求にID、パスワードを含ませる。決済サーバ13は、決済処理（ステップA18）において、IDとパスワードにより利用者の認証を行なえばよい。

【0082】上記に挙げた決済サーバと利用者端末間の3つの認証方法の例は、第2の実施の形態および第3の実施の形態においても実施可能である。

【0083】第1の実施形態において、決済処理に必要な利用者のクレジットカード番号や、口座番号と暗証番号などの利用者口座情報は、第2の決済要求に含ませてもよいが、前述のように、決済サーバ13による利用者認証が可能であれば、決済サーバ13で利用者のクレジットカード番号や口座番号などを保持しておくことも可能である。つまり、第2の決済要求に利用者を識別する識別子を含ませ、決済サーバ13は利用者認証を行なった後、認証に成功すれば利用者識別子をキーに保持したクレジットカード番号や口座番号などを検索し、決済処理を行なえばよい。これは第2の実施の形態または第3

の実施の形態においても同様である。

【0084】上述したように第1乃至第3の実施形態によると、以下の効果を奏する。第1の効果は、利用者のクレジット番号や口座番号を販売店側に秘匿できることである。その理由は、利用者のクレジット番号や口座番号などの秘密情報を利用者から決済サーバに直接、送るためである。第2の効果は、利用者もしくは販売店が決済内容を偽造することができないことである。その理由は、決済サーバが利用者および販売店の双方から決済要求を受け取り、双方の決済内容の突き合わせを行なうことが可能であるためである。第3の効果は、決済サーバが利用者および販売店の双方の認証が可能である。その理由は、決済サーバが利用者および販売店の双方と直接、決済要求を受け付け、認証を行なうことが可能であるためである。第4の効果は、利用者側の暗号化や署名生成のためのプログラムや電子証明書を用意するための負担を軽減する。その理由は、本方式では、利用者側への専用プログラムや電子証明書を必ずしも必要とせず、必要とする場合も、認証子を生成する機能などからなる簡易なもので済むためである。

【0085】

【発明の効果】本発明は以上のように構成され機能するので、これによると、決済サーバが、第1の決済要求を販売店サーバから受信し、第2の決済要求を利用者端末から受信し、続いて、前記第1の決済要求の内容と前記第2の決済要求の内容とを照合し、不整合がない場合に決済処理を行うため、販売店と利用者双方の決済要求が一致していない場合には、決済処理を不成立とさせることで偽造やミスなどによる不正な決済要求を防止することができ、また、決済に必要な利用者の個人情報

利用者端末からのみ送信されても注文内容及び金額の比較で決済を行うことができるため、利用者の個人情報販売店へ漏洩することがなく、従って、利用者の決済に用いる各種の番号等に暗号化を付する等の処理負担を軽減することができる、という、という従来にない優れた電子決済方法を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示すブロック図である。

【図2】本発明の第1の実施の形態の動作の前段を示すシーケンス図である。

【図3】本発明の第1の実施の形態の動作の後段を示すシーケンス図である。

【図4】図1に示す利用者端末にて注文を行う場合に表示される画面の例を示す説明図である。

【図5】図1に示す利用者端末に支払処理要求がなされた場合に表示される画面の例を示す説明図である。

【図6】図1に示す利用者端末から販売店サーバに決済結果を送信するための画面の例を示す説明図である。

【図7】本発明の第2の実施の形態を示すブロック図である。

【図8】本発明の第2の実施の形態の動作の前段を示すシーケンス図である。

【図9】本発明の第2の実施の形態の動作の後段を示すシーケンス図である。

【図10】本発明の第3の実施の形態を示すブロック図である。

【図11】本発明の第3の実施の形態の動作の前段を示すシーケンス図である。

【図12】本発明の第3の実施の形態の動作の後段を示すシーケンス図である。

【図13】本発明の各実施形態に共通するハードウェア資源の構成を示すブロック図である。

【図14】従来の電子決済システムを示すブロック図である。

【符号の説明】

11 販売店サーバ

12 利用者端末

13 決済サーバ

14 通信路

15 通信路

16 通信路

17 金融機関ホストマシン

21 販売店サーバ

22 利用者端末

23 決済サーバ

24 通信路

25 通信路

26 通信路

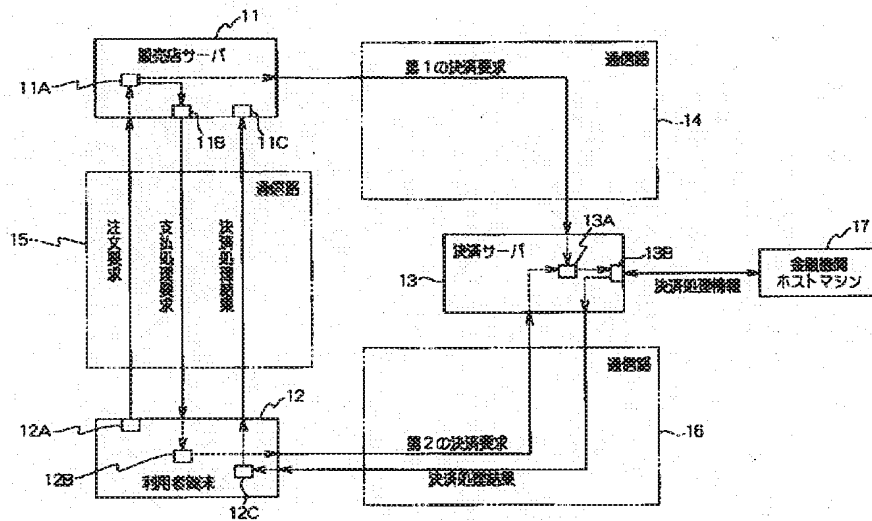
27 金融機関ホストマシン

- 31 販売店サーバ
32 利用者端末
33 決済サーバ
34 通信路

- * 35 通信路
36 通信路
37 金融機関ホストマシン

*

【図1】

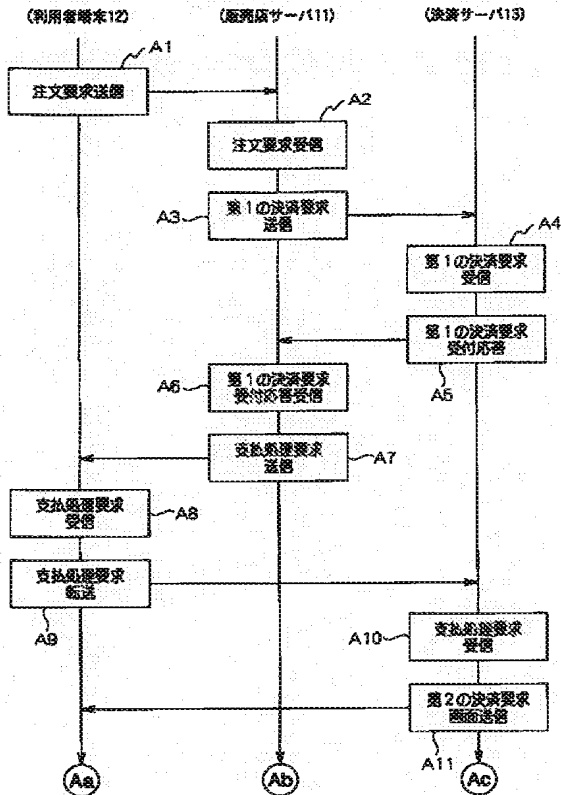


【図4】

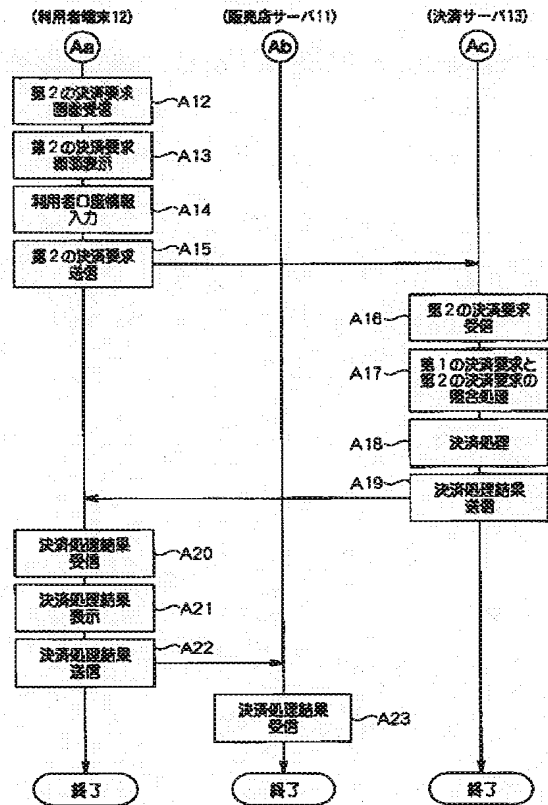
商品名	商品コード	価格
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

お届け先	<input type="text"/>
お名前	<input type="text"/>
ご連絡先	<input type="text"/>

【図2】



【図3】



【図5】

商品名	商品コード	単価	数量	小計
ピーナッツバター	XXXX	¥500	1	¥500
グレープゼリー	YYYY	¥600	1	¥600
消費税				¥55
合計				¥1155

注文番号 1234567890

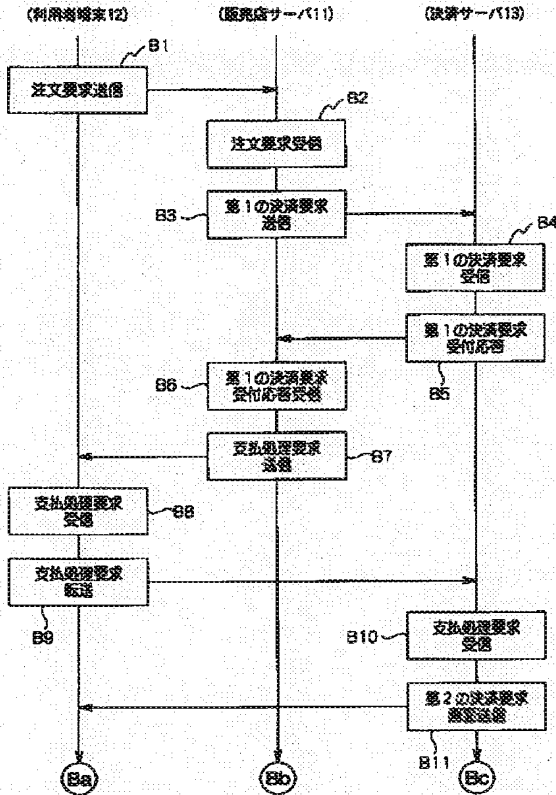
クレジットカード番号

決済処理が終了しました。

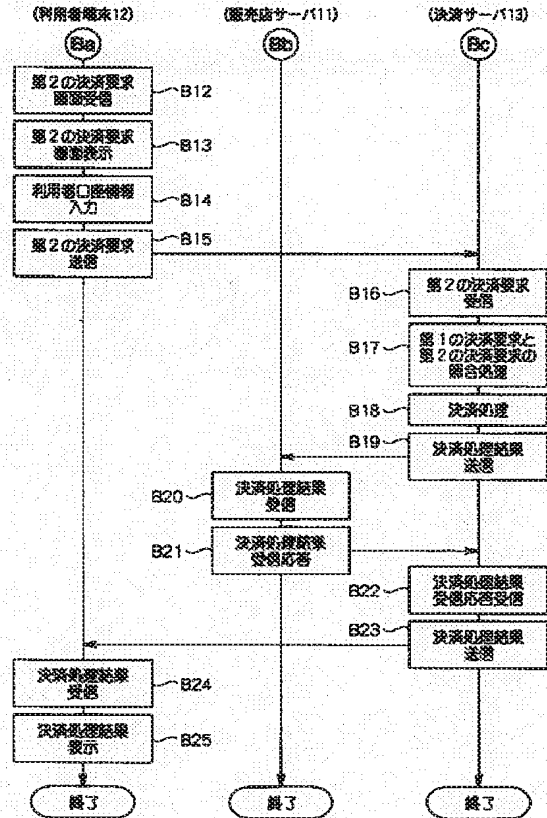
下のボタンをクリックし、決済結果を販売店サーバに送信してください。

[決済結果送信](#)

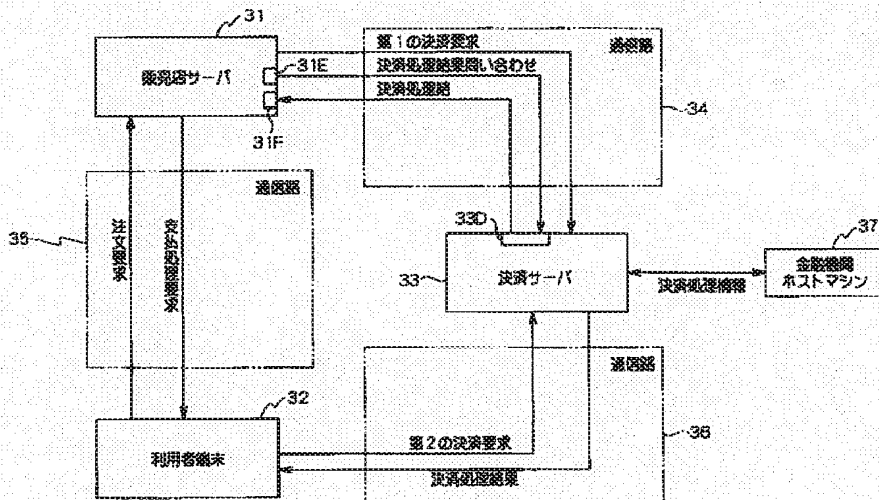
【図8】



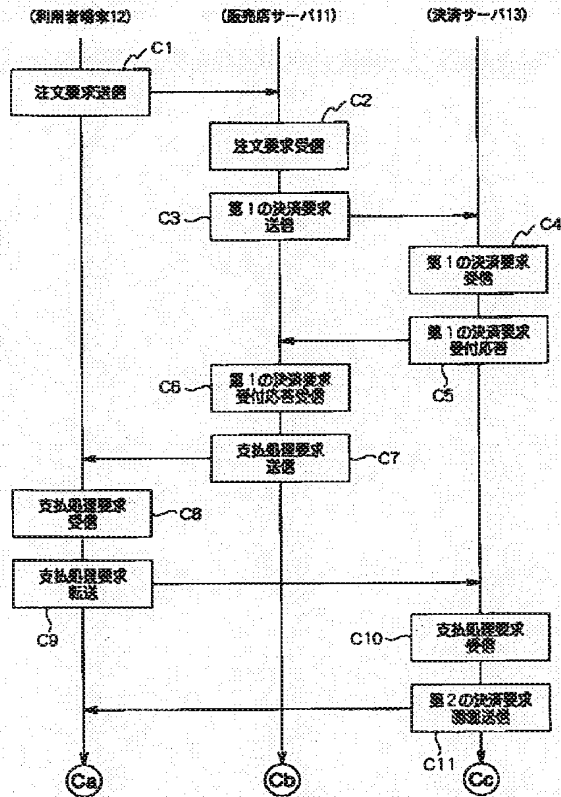
【図9】



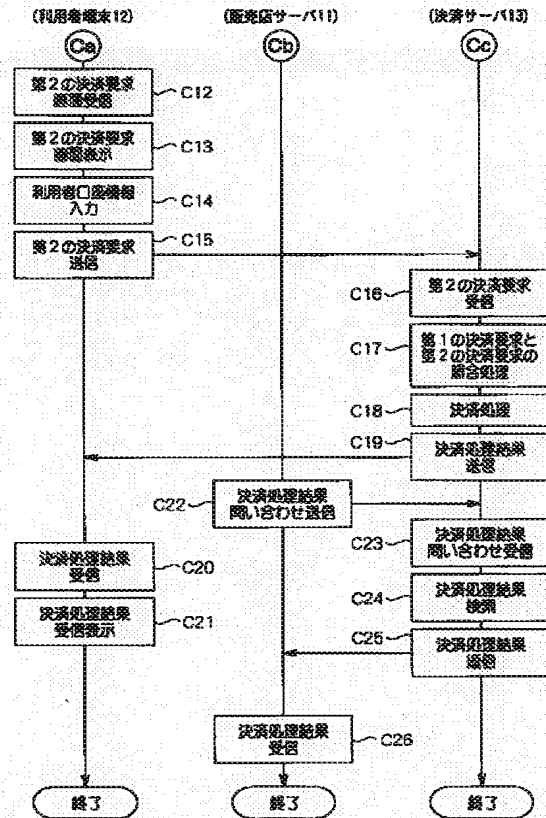
【図10】



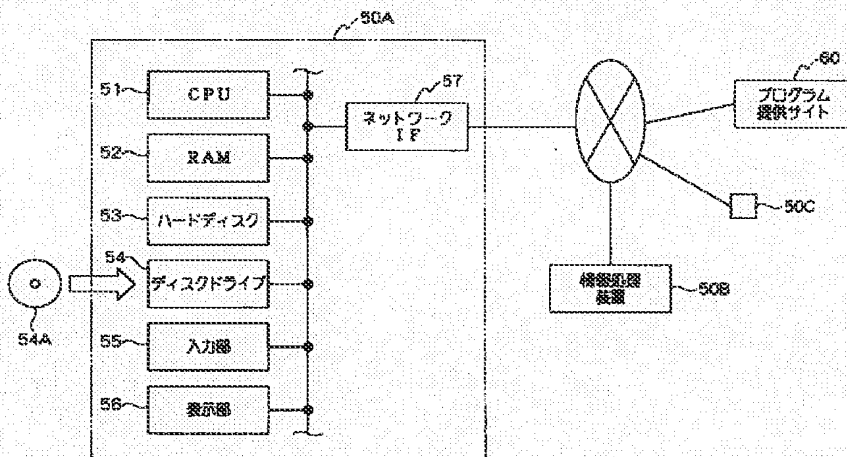
【図11】



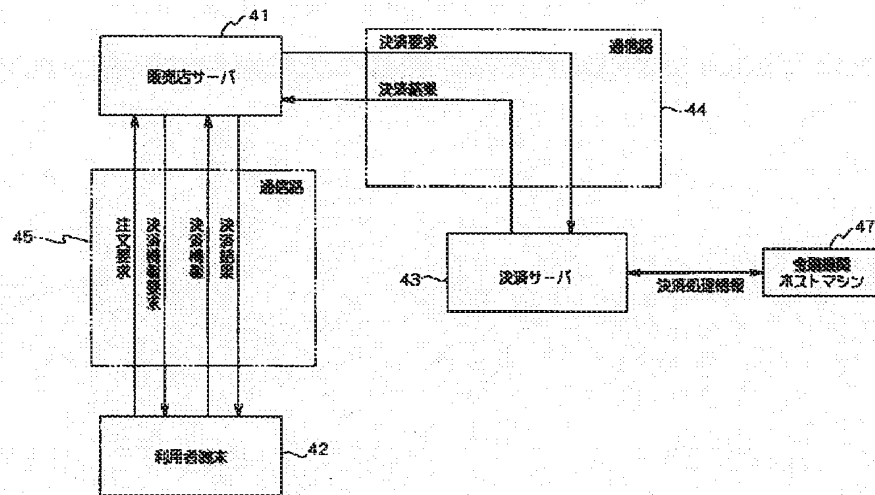
【図12】



【図13】



【図14】



*** NOTICES ***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.** shows the word which can not be translated.**

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]Electronic account settlement method comprising:

A store server connected with a user terminal via a channel.

A step to which it is the electronic account settlement method which performs electronic banking using a settling server connected with said user terminal and said store server via a channel, and said store server receives an article or an order demand of service transmitted from said user terminal.

A step at which said store server transmits a request of settlement processing about said order demand to said settling server as the 1st settlement request.

A step for which a request of settlement processing about an order which said settling server got mixed up with reception of said 1st settlement request, and performed said order demand from said user terminal is received as the 2nd settlement request, A settlement processing step which performs settlement processing when it will compare the contents of said 1st settlement request, and the contents of said 2nd settlement request if said settling server receives said 1st settlement request and said 2nd settlement request, and there is no mismatching.

[Claim 2]Said settlement processing step is provided with a cooperation settlement-of-accounts step which cooperates with a financial institution host machine managed by financial institution, and processes the settlement request concerned, Electronic account settlement method in the claim 1 term case, wherein said settling server is provided with a settlement result transmission step which transmits said settlement processing result to a user terminal and a store server

directly or indirectly following this cooperation settlement-of-accounts step.

[Claim 3]The electronic account settlement method according to claim 1 or 2, wherein said settlement processing step is provided with a settlement-of-accounts abortive step which makes the settlement processing concerned abortive when an order content or the amount of money of said order demand is inharmonious.

[Claim 4]Electronic account settlement method comprising:

A step at which it has a user terminal mutually connected with a channel, a store server, and a settling server, said settling server is further connected with a financial institution host machine, and said user terminal sends an article or an order demand of service to said store server using said channel according to a user's operation.

A step which will send the 1st settlement request to said settling server if said store server receives said order demand, A step which sends a payment processing demand to said user terminal, and a step which said user terminal receives said payment processing demand, and sends the 2nd settlement request to said settling server, If said settling server receives said 1st settlement request and said 2nd settlement request, A settlement processing step which performs settlement processing with said financial institution host machine when the contents of said 1st settlement request and the contents of said 2nd settlement request are compared and there is no mismatching, A step at which the settling server concerned sends a result of said settlement processing to said user terminal, a step which will send a settlement processing result to said store server from said user terminal if said user terminal receives said settlement processing result, and a step from which said store server receives said settlement processing result.

[Claim 5]Electronic account settlement method comprising:

A step at which it has a user terminal mutually connected with a channel, a store server, and a settling server, this settling server is connected with a financial institution host machine, and said user terminal sends an article or an order demand of service to said store server using said channel according to said user's operation.

A step which will send the 1st settlement request to said settling server if said store server receives said order demand, A step which transmits a payment processing demand to said user terminal, and a step which said user terminal receives said payment processing demand, and sends the 2nd settlement request to said settling server, If said settling server receives said 1st settlement request and said 2nd settlement request, A settlement processing step which performs settlement processing with said financial institution host machine when the contents of said 1st

settlement request and the contents of said 2nd settlement request are compared and there is no mismatching, A step at which said settling server sends a result of said settlement processing to said store server, A step from which said store server receives said settlement processing result, a step at which said settling server sends a result of said settlement processing to said user terminal, and a step from which said user terminal receives said settlement processing result.

[Claim 6]Electronic account settlement method comprising:

A step at which it has a user terminal mutually connected with a channel, a store server, and a settling server, this settling server is connected with a financial institution host machine, and said user terminal sends an article or an order demand of service to said store server using said channel according to a user's operation.

A step which will send the 1st settlement request to said settling server if said store server receives said order demand, A step which transmits a payment processing demand to said user terminal, and a step at which said user terminal receives said payment processing demand, and transmits the 2nd settlement request to said settling server, If said settling server receives said 1st settlement request and said 2nd settlement request, A settlement processing step which performs settlement processing with said financial institution host machine when the contents of said 1st settlement request and the contents of said 2nd settlement request are compared and there is no mismatching, Said settling server a step which sends a result of said settlement processing to said user terminal, a step from which said user terminal receives said settlement processing result, and said store server, A step to which a step which asks said settling server a result of said settlement processing, and said settling server which received said inquiry return a result of said settlement processing to said store server, and a step from which said store server receives a result of said settlement processing.

[Claim 7]Exchange a key for performing an attestation child's generation and verification beforehand with said store server and said settling server, and said settling server, Generate an attestation child to said settlement processing result using a key for said attestation child generation, make it contain in said settlement processing result sent to said user terminal, and said user terminal, Receive said settlement processing result, include said attestation child in a settlement processing result sent to said store server, and said store server, The electronic account settlement method according to claim 4 characterized by attesting said settlement

processing result using a key said attestation child who receives said settlement processing result and is contained in said settlement processing result, and for said attestation child verification.

[Claim 8]The electronic account settlement method according to claim 4 or 7 characterized by performing mutual attestation with said settling server and said store server in transmission and reception of said 1st settlement request with a correspondence procedure in which said attestation is possible using a correspondence procedure which can be attested to communication between said store server and said settling server.

[Claim 9]In transmission and reception of said 1st settlement request, and transmission and reception of said settlement processing result using a correspondence procedure which can be attested to communication between said store server and said settling server, The electronic account settlement method according to claim 5 or 6 characterized by performing mutual attestation with said settling server and said store server with a correspondence procedure in which said attestation is possible.

[Claim 10]Decide with said user and said settling server on a key for performing an attestation child's generation and verification beforehand, and a user's identifier which identifies said user, and said user terminal, Generate an attestation child to said 2nd settlement request using a key for said attestation child generation, include said attestation child and said user's identifier in said 2nd settlement request, and said settling server, From said user's identifier contained in said 2nd settlement request, in said settlement processing step, specify a key for said attestation child verification, and with a key for said attestation child verification with said attestation child. Electronic account settlement method of any 1 statement of claims 4 thru/or 9 performing attestation of said user and said 2nd settlement request.

[Claim 11]Exchange a key for performing an attestation child's generation and verification beforehand with said user and said settling server, and said settling server, Generate an attestation child to a result of said settlement processing using a key for said attestation child generation, make it contain in a result of said settlement processing, and said user terminal, Electronic account settlement method of any 1 statement of claims 4 thru/or 10 characterized by performing attestation of said settling server and said settlement processing result in a step which receives said settlement processing result with a key an attestation child to a result of said settlement processing, and for said attestation child verification.

[Claim 12]In transmission and reception as a result of said 2nd settlement request and

said settlement processing using a correspondence procedure which can be attested to communication between said user terminal and said settling server, Electronic account settlement method of any 1 statement of claims 4 thru/or 9 characterized by performing mutual attestation with said user and a settling server with a correspondence procedure in which said attestation is possible.

[Claim 13]Decide on a user's identifier and user confidential information between said user and said settling server beforehand, and to said 2nd settlement request including said user's identifier and said user confidential information said settling server, Electronic account settlement method of any 1 statement of claims 4 thru/or 9 characterized by attesting a user by said user's identifier and said user confidential information in said settlement processing step.

[Claim 14]Electronic account settlement method of any 1 statement of claims 6 thru/or 13, wherein it includes user account information required for settlement processing in said 2nd settlement request and said settling server performs settlement processing using said user account information.

[Claim 15]The electronic account settlement method according to claim 10, 12, or 13 when user account information required for settlement processing is held with said settling server, and said user authentication is successful, wherein said settling server performs settlement processing by said held user account information.

[Claim 16]If it is connected with a user terminal and a settling server with a channel and an order demand is received from said user terminal, A means to send the 1st settlement request including information about said order content and the settlement request amount of money to said settling server, A store server provided with a means to send a payment processing demand which includes information about said order content and said settlement request amount of money in said user terminal, and a means to receive a settlement processing result returned from said user terminal.

[Claim 17]If it is connected with a user terminal and a settling server with a channel and an order demand is received from said user terminal, A means to send the 1st settlement request including information about said order content and the settlement request amount of money to said settling server, A store server containing a means to send a payment processing demand which furthermore includes information about said order content and said settlement request amount of money in said user terminal, and a means to receive a settlement processing result returned from said settling server.

[Claim 18]If it is connected with a user terminal and a settling server with a channel and an order demand is received from said user terminal, A means to send the 1st settlement request including information about said order content and the settlement

request amount of money to said settling server, A means to send a payment processing demand which furthermore includes information about said order content and said settlement request amount of money in said user terminal, A store server containing a means to ask said settling server a result of said 1st settlement request, and a means to receive a settlement processing result returned from said settling server.

[Claim 19]With an attestation child of said settling server to a settlement processing result which exchanges a key for performing an attestation child's generation and verification beforehand with said settling server, and is included in said settlement processing result, and a key for said attestation child verification. The store server according to claim 16 performing attestation of said settling server and said settlement processing result.

[Claim 20]In transmission and reception of said 1st settlement request, and transmission and reception of said settlement processing result using a correspondence procedure which can be attested to communication between said settling servers, A store server of any 1 statement of claims 16 thru/or 18 characterized by performing mutual attestation with said settling server and said store server with a correspondence procedure in which said attestation is possible.

[Claim 21]A settling server comprising:

A means for it to be connected with a user terminal and a store server with a channel, to be further connected with a financial institution host machine, and to receive the 1st settlement request from said store.

A means to receive the 2nd settlement request from said user terminal.

A means by which said financial institution host machine performs settlement processing when the contents of settlement of accounts in said 1st settlement request and said 2nd settlement request are compared and there is no mismatching.

A means to send a result of said settlement processing to said user terminal.

[Claim 22]A settling server comprising:

A means for it to be connected with a user terminal and a store server with a channel, to be further connected with a financial institution host machine, and to receive the 1st settlement request from said store.

A means to receive the 2nd settlement request from said user terminal.

A means by which said financial institution host machine performs settlement processing when the contents of settlement of accounts in said 1st settlement request and said 2nd settlement request are compared and there is no mismatching.

A means to send a result of said settlement processing to said user terminal, and a means to send said settlement processing result to said store server further.

[Claim 23]A settling server comprising:

A means for it to be connected with a user terminal and a store server with a channel, to be further connected with a financial institution host machine, and to receive the 1st settlement request from said store.

A means to receive the 2nd settlement request from said user terminal.

A means by which said financial institution host machine performs settlement processing when the contents of settlement of accounts in said 1st settlement request and said 2nd settlement request are compared and there is no mismatching.

A means to send a result of said settlement processing to said user terminal, and a means to return said settlement processing result to said store server if an inquiry as a result of said 1st settlement request is received from said store server.

[Claim 24]The settling server according to claim 21 exchanging a key for performing an attestation child's generation and verification beforehand with said store server, generating an attestation child of said settling server to said settlement processing result using a key for said attestation child generation, and including in a result of said settlement processing.

[Claim 25]The settling server according to claim 21 or 24 characterized by attesting said store server in transmission and reception of said 1st settlement request with a correspondence procedure in which said attestation is possible using a correspondence procedure which can be attested to communication with said store server.

[Claim 26]The settling server according to claim 22 or 23 characterized by attesting said store server with a correspondence procedure in which said attestation is possible in transmission and reception of said 1st settlement request, and transmission and reception of said settlement processing result using a correspondence procedure which can be attested to communication with said store server.

[Claim 27]In [decide on a key for performing an attestation child's generation and verification beforehand with said user, and a user's identifier which identifies said user, and] said settlement processing function, A settling server of any 1 statement of claims 21 thru/or 26 performing attestation of a user and a settlement request with a key for said attestation child verification with an attestation child who specifies a key

for said attestation child verification from said user's identifier contained in said 2nd settlement request, and is contained in said 2nd settlement request.

[Claim 28]A settling server of any 1 statement of claims 21 thru/or 27 exchanging a key for performing an attestation child's generation and verification beforehand with said user, generating an attestation child to a result of said settlement processing using a key for said attestation child generation, and including in a result of said settlement processing.

[Claim 29]In transmission and reception as a result of said 2nd settlement request and said settlement processing using a correspondence procedure which can be attested to communication between said user terminal and said settling server, A settling server of any 1 statement of claims 21 thru/or 28 characterized by performing mutual attestation with said settling server and said user with a correspondence procedure in which said attestation is possible.

[Claim 30]In [decide on a user's identifier and user confidential information between said user and said settling server beforehand, and] said settlement processing function, A settling server of any 1 statement of claims 21 thru/or 29 attesting a user by said user's identifier contained in said 2nd settlement request, and said user confidential information.

[Claim 31]A settling server of any 1 statement of claims 21 thru/or 30 characterized by performing said settlement processing function using user account information required for settlement processing included in said 2nd settlement request.

[Claim 32]The settling server according to claim 27, 29, or 30 performing settlement processing with said settlement processing function using said user account information which held user account information required for settlement processing when it succeeded in maintenance punishment and said user authentication beforehand.

[Claim 33]An electronic clearing system comprising:

A means by which it has a user terminal mutually connected with a channel, a store server, and a settling server, said settling server is further connected with a financial institution host machine, and a user sends an article or an order demand of service to said store server using said user terminal and said channel.

A means to send the 1st settlement request to said settling server if said store server receives said order demand, A means to send a payment processing demand to said user terminal furthermore, and a means by which said user terminal receives said payment processing demand, and sends the 2nd settlement request to said settling server, If said settling server receives said 1st settlement request and said 2nd

settlement request, A settlement processing means which performs settlement processing with said financial institution host machine when the contents of said 1st settlement request and the contents of said 2nd settlement request are compared and there is no mismatching, A means to send a result of said settlement processing to said user terminal, a means to send a settlement processing result to said store server from said user terminal if said user terminal receives said settlement processing result, and a means by which said store server receives said settlement processing result.

[Claim 34]An electronic clearing system comprising:

A means by which it has a user terminal mutually connected with a channel, a store server, and a settling server, said settling server is further connected with a financial institution host machine, and a user sends an article or an order demand of service to said store server using said user terminal and said channel.

A means to send the 1st settlement request to said settling server if said store server receives said order demand, A means to transmit a payment processing demand to said user terminal furthermore, and a means by which said user terminal receives said payment processing demand, and sends the 2nd settlement request to said settling server, If said settling server receives said 1st settlement request and said 2nd settlement request, A settlement processing means which performs settlement processing with said financial institution host machine when the contents of said 1st settlement request and the contents of said 2nd settlement request are compared and there is no mismatching, A means by which said settling server furthermore sends a result of said settlement processing to said store server, a means by which said store server receives said settlement processing result, a means by which said settling server sends a result of said settlement processing to said user terminal further, and a means by which said user terminal receives said settlement processing result.

[Claim 35]An electronic clearing system comprising:

A means by which it has a user terminal mutually connected with a channel, a store server, and a settling server, said settling server is further connected with a financial institution host machine, and a user sends an article or an order demand of service to said store server using said user terminal and said channel.

A means to send the 1st settlement request to said settling server if said store server receives said order demand, A means to transmit a payment processing demand to

said user terminal furthermore, and a means by which said user terminal receives said payment processing demand, and transmits the 2nd settlement request to said settling server, If said settling server receives said 1st settlement request and said 2nd settlement request, A settlement processing means which performs settlement processing with said financial institution host machine when the contents of said 1st settlement request and the contents of said 2nd settlement request are compared and there is no mismatching, A means to send a result of said settlement processing to said user terminal furthermore, a means by which said user terminal receives said settlement processing result, and said store server, A means by which a means to ask said settling server a result of said settlement processing, and said settling server which received said inquiry return a result of said settlement processing to said store server, and a means by which said store server receives a result of said settlement processing.

[Claim 36]Exchange a key for performing an attestation child's generation and verification beforehand with said store server and said settling server, and said settling server, Generate an attestation child to said settlement processing result using a key for said attestation child generation, make it contain in said settlement processing result sent to said user terminal, and said user terminal, Receive said settlement processing result, include said attestation child in a settlement processing result sent to said store server, and said store server, The electronic clearing system according to claim 33 characterized by attesting said settlement processing result using a key said attestation child who receives said settlement processing result and is contained in said settlement processing result, and for said attestation child verification.

[Claim 37]In transmission and reception of said 1st settlement request using a correspondence procedure which can be attested to communication between said store server and said settling server, The electronic clearing system according to claim 33 or 36 characterized by performing mutual attestation with said settling server and said store server with a correspondence procedure in which said attestation is possible.

[Claim 38]In transmission and reception of said 1st settlement request, and transmission and reception of said settlement processing result using a correspondence procedure which can be attested to communication between said store server and said settling server, Claim 34 characterized by performing mutual attestation with said settling server and said store server with a correspondence

procedure in which said attestation is possible, or an electronic clearing system given [any 1] in 35.

[Claim 39]Decide with said user and said settling server on a key for performing an attestation child's generation and verification beforehand, and a user's identifier which identifies said user, and said user terminal, Generate an attestation child to said 2nd settlement request using a key for said attestation child generation, include said attestation child and said user's identifier in said 2nd settlement request, and said settling server, From said user's identifier contained in said 2nd settlement request, in said settlement processing means, specify a key for said attestation child verification, and with a key for said attestation child verification with said attestation child. An electronic clearing system of any 1 statement of claims 33 thru/or 38 performing attestation of said user and said 2nd settlement request.

[Claim 40]Exchange a key for performing an attestation child's generation and verification beforehand with said user and said settling server, and said settling server, Generate an attestation child to a result of said settlement processing using a key for said attestation child generation, make it contain in a result of said settlement processing, and said user terminal, An electronic clearing system of any 1 statement of claims 33 thru/or 39 characterized by performing attestation of said settling server and said settlement processing result in a means to receive said settlement processing result, with a key an attestation child to a result of said settlement processing, and for said attestation child verification.

[Claim 41]In transmission and reception as a result of said 2nd settlement request and said settlement processing using a correspondence procedure which can be attested to communication between said user terminal and said settling server, An electronic clearing system of any 1 statement of claims 33 thru/or 38 characterized by performing mutual attestation with said user and a settling server with a correspondence procedure in which said attestation is possible.

[Claim 42]Decide on a user's identifier and user confidential information between said user and said settling server beforehand, and to said 2nd settlement request including said user's identifier and said user confidential information said settling server, An electronic clearing system of any 1 statement of claims 33 thru/or 38 characterized by attesting a user by said user's identifier and said user confidential information in said settlement processing means.

[Claim 43]An electronic clearing system of any 1 statement of claims 33 thru/or 42, wherein it includes user account information required for settlement processing in said 2nd settlement request and said settling server performs settlement processing

using said user account information.

[Claim 44]The electronic clearing system according to claim 39, 41, or 42 when user account information required for settlement processing is held with said settling server, and said user authentication is successful, wherein said settling server performs settlement processing by said held user account information.

[Claim 45]A recording medium which recorded a store server program which performs the contents of processing of a store server of any 1 of said claims 16 thru/or 19 using an information processor.

[Claim 46]A transmission medium which transmits a store server program which performs the contents of processing of a store server of any 1 of said claims 16 thru/or 20 using an information processor via a channel.

[Claim 47]A recording medium which recorded a settlement-of-accounts server program which performs the contents of processing of any 1 settling server of said claims 21 thru/or 32 using an information processor.

[Claim 48]A transmission medium which transmits a settlement-of-accounts server program which performs the contents of processing of said claim 21 thru/or claim 32 any 1 settling server using an information processor.

[Claim 49]A storage which memorized a program for electronic banking for performing electronic banking using a store server characterized by comprising the following connected with a user terminal and this user terminal via a channel, and a settling server connected with said user terminal and said store server via a channel.

The 1st reception command that makes a settlement request of the order concerned receive as the 1st settlement request when said program for electronic banking has an order to said store from a user who is a holder of said user terminal as instructions which operate said settling server.

The 2nd reception command that makes a settlement request of said order receive from said user terminal.

Settlement request collation instructions which make the contents of said 1st settlement request, and the contents of said 2nd settlement request compare according to reception with said 1st settlement request and said 2nd settlement request.

Settlement processing instructions which perform the settlement processing concerned when there is no mismatching in the contents of said 1st and 2nd settlement requests according to these settlement request collation instructions.

[Claim 50]A storage which memorized a program for electronic banking for performing

electronic banking using a store server characterized by comprising the following connected with a user terminal and this user terminal via a channel, and a settling server connected with said user terminal and said store server via a channel. Instructions to which said settling server is made to transmit as the 1st settlement request with an identification number which identifies order content concerned and the order concerned, and a user when said program for electronic banking receives an order from a user of said user terminal as instructions which operate said store server. Instructions which make said order content transmit to said user terminal as a payment processing demand. Instructions which make a result of said settlement of accounts receive with an identification number which discriminates said order and a user from said settling server or said user terminal.

[Claim 51] A storage which memorized a program for electronic banking for performing electronic banking using a store server characterized by comprising the following connected with a user terminal and this user terminal via a channel, and a settling server connected with said user terminal and said store server via a channel. A payment request instruction reception command which makes an identification number which discriminates order content concerned and the order concerned, and a user from said store server which received an order from a user of the user terminal concerned as instructions to which said program for electronic banking operates said user terminal receive as payment request instructions. 2nd settlement request transmission commands that makes the 2nd settlement request for requiring settlement of the payment request concerned of said settling server according to reception of this payment request instruction reception command transmit to said settling server with an identification number of said order and a user. A settlement result reception command which makes a settlement result of the order content concerned receive from a settling server which operates according to these 2nd settlement request transmission commands.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the electronic account settlement method and the electronic clearing system which perform settlement of the article which received the order from the user, or the price to service via a network.

[0002]

[Description of the Prior Art] The block diagram of the conventional electronic clearing system which settles the article which received the order from the user, or the price to service is shown in drawing 14 using networks, such as the Internet. The user who is a buyer sends an order demand to a seller's store server 41 using the user terminal 42 and the channel 45. The store server 41 which received this transmits a demand of user account information, such as a user's credit card number and a bank account number, to the user terminal 42. A user sends the above-mentioned user account information to the store server 41 using the user terminal 42.

[0003] The store server 41 sends out the settlement request based on the above-mentioned user account information to the settling server 43 through the channel 44. The settling server 43 processes this settlement request by cooperation with a financial institution host machine, and returns that settlement processing result to the store server 41. In the store server 41, the above-mentioned settlement processing result is returned to the user terminal 42 through the channel 45.

[0004] The purchase of goods or service can be settled by composition shown in this drawing 14, without using cash.

[0005]

[Problem(s) to be Solved by the Invention] However, when accounts was settled by the information flow which the above-mentioned conventional example depends, it was exposed of user account information, such as a user's credit card number and a bank account number, to the store server by the side of a seller, and there was inconvenience that there was a danger of being abused for the seller side. Since a settlement amount goes to a financial institution only from the seller side, there is a danger that the amount of money will be altered.

[0006] In order to prevent this, there are protocols, such as SET and SECE. It is possible for encryption of user account information, electronic signature grant to a settlement amount, etc. to be performed, and to avoid the above-mentioned danger in these protocols. However, in order to perform encryption and generation of an electronic signature, it is necessary to prepare the program and electronic certificate

for encryption or signature generating for the user side, and in order to prepare it, the burden and expense burden of work will be forced upon a user.

[0007]

[Objects of the Invention]Then, the purpose of this invention eases encryption, the program for signature generating, the burden by the side of the user who prepares an electronic certificate, and the burden of hardware resources, Moreover, user account information, such as a user's credit card number and a bank account number, can be kept secret from the seller side, and it is in a user providing intelligible electronic account settlement method about safety.

[0008]

[Means for Solving the Problem]Then, a store server connected with a user terminal via a channel in this invention, It is the electronic account settlement method which performs electronic banking using a settling server connected with said user terminal and said store server via a channel, It has a step to which a store server receives an article or an order demand of service transmitted from said user terminal, and a step at which a store server transmits a request of settlement processing about said order demand to said settling server as the 1st settlement request. Then, a step for which a request of settlement processing about an order which a settling server got mixed up with reception of said 1st settlement request, and performed said order demand from said user terminal is received as the 2nd settlement request, Composition that a settling server was provided with a settlement processing step which will perform settlement processing when the contents of said 1st settlement request and the contents of said 2nd settlement request are compared and there is no mismatching if said 1st settlement request and said 2nd settlement request are received is taken. It is going to attain the purpose which this mentioned above.

[0009]In this invention, if an application of a commercial transaction is made in a user and a store, a settlement request will be performed from both sides of a store server and a user server to a settling server. That is, a settling server receives the 1st settlement request from a store server, and receives the 2nd settlement request from a user terminal. If the 1st settlement request and said 2nd settlement request are received, a settling server compares the contents of said 1st settlement request, and the contents of said 2nd settlement request, and when there is no mismatching, it will perform settlement processing (settlement processing step). For this reason, settlement processing becomes abortive when a settlement request of both a store and a user is not in agreement. Since personal information of a user required for settlement of accounts can be settled by comparison of an order content and the

amount of money even if transmitted only from a user terminal, a user's personal information does not reveal it to a store.

[0010]According to a desirable embodiment, various composition can be taken about transfer of a settlement result. A settlement request is advanced by the 1st electronic account settlement method from both sides of a store server and a user terminal to a settling server, and user account information is included only in a settlement request from a user terminal by it. A settlement processing result by a settling server is returned to a store server via a user terminal. A user gives an order demand to a store server using a user terminal, and, more specifically, in response, a store server advances a settlement request to both sides of a settling server and a user terminal. A user receives a settlement request using a user terminal, and sends a settlement request including user account information, such as his credit card number and a bank account number, to a settling server. A settling server does not have a difference in a request content from both sides, or settlement processing is performed after a check, a settlement processing result is returned to a user terminal, and a user terminal returns a settlement processing result to a store server.

[0011]The 2nd electronic account settlement method and electronic clearing system advance a settlement request from both sides of a store server and a user terminal to a settling server like the 1st electronic account settlement method, and user account information is included only in a settlement request from a user terminal. A different point from the 1st electronic account settlement method is a point of returning a settlement processing result by a settling server to a user terminal and both sides of a store server directly from a settling server.

[0012]The 3rd electronic account settlement method and electronic clearing system advance a settlement request from both sides of a store server and a user terminal to a settling server like the 1st electronic account settlement method, and user account information is included only in a settlement request from a user terminal. A settling server which a settlement processing result according [a different point from the 1st electronic account settlement method] to a settling server was returned to a user terminal from a settling server, and a store server asked a settling server a settlement processing result separately, and received the inquiry is a point which notifies a settlement processing result to a store server.

[0013]

[Embodiment of the Invention]Next, the electronic account settlement method of this invention and the embodiment of an electronic clearing system are described in detail with reference to drawings.

[0014]When <1st embodiment> drawing 1 is referred to, a 1st embodiment of the electronic account settlement method of this invention comprises the following:

Store server 11.

User terminal 12.

Settling server 13.

The channel 14 which connects the settling server 13 and the store server 11, the channel 15 which connects the user terminal 12 to the store server 11, the channel 16 which connects the settling server 13 to the user terminal 12, and the financial institution host machine 17 connected to the settling server 13.

[0015]The channel 14, the channel 15, and the channels 16 may be general-purpose networks, such as the Internet, and may be communication lines for exclusive use etc. You may be a channel with which the channel 14 and the channel 15 differ from the channel 16, and may be the same channels, such as the Internet, altogether. Each is good also as a mobile radio communication network and a complex communications network by the Internet etc.

[0016]The store server 11 is used by a product, the vender of service, or its proxy, and is constituted by information processors, such as a workstation server. The store server 11 may be a server for single stores, and may be a common server for two or more stores. The store server 11 is provided with the function to receive the order demand from a user terminal, via the channel 15. When an order demand is received, it has the function to send the 1st settlement request to a settling server via the channel 14, and the function to send a payment processing demand to a user terminal via the channel 15. It has the function to receive a settlement processing result from a user terminal via the channel 15. It can also be constituted from two or more information processors that it performs the function to receive an order demand, and a settlement request and the function, as for which a result acquires with a separate information processor although the store server 11 may comprise a single information processor etc.

[0017]A settlement request here refers to a recognition check (the credit check in the case of credit settlement, and the balance confirmation of bank settlement of accounts) and payment collection of an article or the price to service. It can also think including revocation of approval, refund, etc. widely.

[0018]The user terminals 12 are information processors, such as a personal computer, a personal digital assistant, an information home appliance. A function required for the user terminal 12 to the 1st The store server 11 and the settling server 13, an order

demand, and a settlement request, The settlement result display function which displays the settlement processing result from the contents and the settling server 13 of a settlement request from the store server 11 on the communication function which transmits and receives a settlement processing result, and the 2nd for a user's check, It is an inputting function for 3rd inputting user account information, such as an order content, a credit card number, and a bank account number. If the communications network 15 and the communications network 15 are the Internet, it is the function which could realize these functions with a personal computer and browser software, and it has as standard in many personal digital assistants and information home appliances.

[0019]When the user terminals 12 are a personal computer, a personal digital assistant, and an information home appliance, an order can be placed using each apparatus. That is, an order can be transmitted to a store server by operating the user terminal 12. If a personal digital assistant is used, it can also use for the payment for the purchase of the article in a actual store, offer of service, etc. In this case, a user can be realized by telling a store about the number of a personal digital assistant, etc., or forming the apparatus which can transmit and receive a personal digital assistant and data in the register of a store, etc. A store server transmits a payment processing demand to the user terminal concerned.

[0020]The settling server 13 is used by settlement-of-accounts entrepreneurs, such as a credit card company and a bank, or the proxy of those, and is constituted by information processors, such as a workstation server. The settling server is provided with the function to receive the 1st settlement request from the store server 11 via the channel 14, and the function to receive the 2nd settlement request from the user terminal 12 via the channel 15. A user individual's user account information receives a credit card number, a bank account number, etc. required for settlement of accounts by the 2nd settlement request from the user terminal 12. From both to a settlement request, the settling server 13 recognizes the settlement request from both to be a thing to the same order by this identification information including the same identification information that specifies an order.

[0021]The settling server 13 performs settlement processing based on the 1st settlement request and 2nd settlement request. This is performed by exchanging separately the information about the financial institution host machine 17 and settlement processing which were connected via a financial network etc. The settling server 13 is provided with the function which transmits the result of settlement processing to the user terminal 12 connected via the channel 16. As for constituting

from two or more information processors, although the settling server 13 may comprise a single information processor, it is also possible for a separate information processor to perform a communication portion with the store server 11, a communication portion with the user terminal 12, and a communications processing portion with a financial institution host machine etc.

[0022]Next, the typical example of operation in a 1st embodiment of this invention is explained with reference to drawing 2 thru/or drawing 6. Here, the channel 15 and the channel 16 presuppose that it is the Internet, and use the user terminal 12 as the terminal equipment which has a browser function of the Internet. Processing of drawing 2 and drawing 3 is continuing in the numerals Aa, Ab, and Ac.

[0023]First, in order to receive the order demand from the user terminal 12 via the Internet (channel 15), a screen which is illustrated to the store server 11 at drawing 4 is prepared for the store server 11. Using the user terminal 11, the user who is a buyer connects with the store server 11 via the Internet (channel 15), displays a screen which is illustrated to drawing 4, and chooses or inputs the name of goods to order, a bar code, and the number. Furthermore, information, including a receiver's address, a name, a contact, etc., is inputted. A user sends an order demand to the store server 11 by operating the order execution button of a screen as shows input sushi and drawing 4 necessary information (drawing 2 step A1). This is realizable by methods, such as POST of an HTTP protocol. Information, including the name of the goods which the user inputted, a bar code, the number, a receiver's address, a name, a contact, etc., shall be included in an order demand here.

[0024]The store server 11 receives the above-mentioned order demand by CGI script etc. (Step A2). A store server assigns the identification number for specifying an order here. If required, processing required for merchandise management, such as reservation of stock, and processing required for shipping products will be performed.

[0025]Subsequently, the store server 11 sends the 1st settlement request to the settling server 13 via the channel 14 (step A3). The 1st settlement request contains the above-mentioned identification number for specifying an order. Information, including a trade name, a unit price, the number, etc., is included as an order content. The Hash value (value compressed on the other hand with the tropism function) of an order content may be sufficient as this. If the channel 14 is the Internet, transmission of this 1st settlement request is realizable by methods, such as POST of an HTTP protocol.

[0026]The settling server 13 receives the 1st above-mentioned settlement request (step A4). This is realizable by CGI script etc., if the channel 14 is the Internet. The

settling server 13 which received the 1st settlement request holds this demand inside. If required, the settling server 13 which received the 1st settlement request will return the response (response) of demand reception to the store server 11 (step A5), and the store server 11 will receive this (Step A6).

[0027]Although the store server was assigning the identification number which specifies an order in the explanation so far, when the settling server 13 receives the 1st settlement request, the method of assigning the identification number which specifies an order and notifying to a store server as a response of demand reception may be sufficient as the settling server 13.

[0028]Subsequently, the store server 11 transmits a payment processing demand to the user terminal 12 (Step A7). This is realizable by sending as a response of the order demand sent by methods, such as POST of an HTTP protocol. Information, including a trade name, a unit price, the number, etc., is included in this payment processing demand as the above-mentioned identification number for specifying an order, and an order content.

[0029]The user terminal 12 receives a payment processing demand from the store server 11 as a response of an order demand (Step A8), and transmits this to the settling server 13 (step A9). Even if this uses the function of an HTTP protocol of redirection, it is realizable, or a screen is returned as a payment processing demand and also making a payment processing demand transmit to the settling server 13 can be realized by making a user click the button on the screen.

[0030]The settling server 13 receives the transmitted payment processing demand (Step A10), and returns a display and input screen of the 2nd settlement request to the user terminal 13 based on this (Step A11). A display and input screen of this 2nd settlement request are illustrated to drawing 5. A trade name, a bar code, a unit price, the number, the total amount, etc. which were ordered can be displayed on this screen. The identification number which specifies an order is also included. The entry column of user account information and a settlement-of-accounts execution button are included. Although the input column of a credit card number is illustrated as an example at the time of a credit card transaction in drawing 5, in bank settlement of accounts, it becomes input columns, such as an account number and a password.

[0031]The user terminal 12 receives a display and input screen of the 2nd settlement request from the settling server 13 (Step A12 of drawing 3), and displays this (Step A13).

[0032]Although the payment processing demand was transmitted to the settling server 13 by explanation of Step A13 from the above-mentioned step A9 and the

practice which prepares a display and input screen of the 2nd settlement request with the settling server 13 was explained, There is also a way the store server 11 sends a payment processing demand to the user terminal 12 as a display and an input screen of the 2nd settlement request at Step A7. The store server 11 starts the special software by the side of the user terminal 12 at Step A7, and there is also a way the special software prepares a display and input screen of the 2nd settlement request. Step A12 becomes unnecessary from step A9 in these cases.

[0033]A user checks an order content in a display and input screen of this 2nd settlement request, and if correct, he will write down necessary information in entry columns, such as a credit card number, an account number, a password, as user account information (Step A14).

[0034]If a user inputs user account information and clicks a settlement-of-accounts execution button, the 2nd settlement request will be sent to the settling server 13 via the channel 16 (Step A15). This is realizable by methods, such as POST of an HTTP protocol. User account information, such as the name of the goods which the user ordered, a bar code, the number, an identification number that specifies an order and a credit card number which the user inputted, an account number, a password, is included in the 2nd settlement request here.

[0035]The settling server 13 receives the 2nd above-mentioned settlement request by CGI script etc. (Step A16).

[0036]The settling server 13 which received the 2nd settlement request compares the contents of the demand with the 1st settlement request received previously (Step A17). When there are two or more orders simultaneously, although the settling server 13 will hold two or more 1st settlement requests, it can specify the 1st corresponding settlement request with the identification number which specifies an order.

Processing of collation compares whether there is any difference in the kind of goods, the number, the amount of money, etc. by the 1st settlement request and 2nd settlement request. Thereby, a store or a user alters an order content and can prevent performing an unjust order or settlement of accounts.

[0037]When mismatching, such as abnormalities, is not detected by the above-mentioned collation, the settling server 13 performs settlement processing (Step A18). Based on user account information included in the 1st settlement request, such as a user's credit card number and an account number, this, Settlement processing is performed and it can realize by exchanging separately the information about the financial institution host machine 17 and settlement processing which were connected via a financial network etc. The account information (bank account number

etc.) by the side of the seller who receives a price may be received from the store server 11 by the 1st settlement request, and may be beforehand held with the settling server 13.

[0038]After settlement processing finishes, the settling server 13 transmits a settlement processing result to the user terminal 12 (Step A19). This is realizable by returning a HTML screen as a response of the 2nd settlement request sent by methods, such as POST of an HTTP protocol.

[0039]The user terminal 12 receives and (Step A20) displays this settlement processing result screen (Step A21). The example of this screen is shown in drawing 6. A user checks the result of settlement processing here, and if the button in which a user sends a settlement processing result to a store server is further clicked according to directions of a screen, he will transmit a settlement processing result to a store server (Step A22). This is realizable by methods, such as POST of an HTTP protocol. The store server 11 receives the settlement processing result sent from the user terminal 12 (Step A23), and performs required processing of shipping products etc.

[0040]Although a user checks a settlement processing result on the screen illustrated by drawing 6 returned at Step A19 from the settling server 13 and the example to which a settlement processing result returns to the store server 11 by a user's button grabbing explains in the above-mentioned explanation, Transmitting directly the settlement processing result returned to the user terminal 12 from the settling server 13 to the store server 11 with the function of an HTTP protocol of redirection as other practices, a user also has a method of checking a settlement processing result on the screen of the response from the store server 11.

[0041]According to a 1st above-mentioned embodiment, a settlement processing result is returned to the store server 11 via the user terminal 12. Therefore, although a malicious user may forge a settlement processing result and may perform injustice, it is detectable by the following methods etc.

[0042]First, the key for the store server 11 and the settling server 13 to perform an attestation child's generation and verification beforehand is exchanged. An attestation child here refers to MAC using a secret key cryptosystem (symmetrical key code), the digital signature using public key encryption, etc.

[0043]The settling server 13 generates the attestation child to a settlement processing result using the key for the above-mentioned attestation child generation, and is made to contain him in said settlement processing result sent to the user terminal 12. The user terminal 13 receives the settlement processing result from the

settling server 13, and includes the aforementioned attestation child in the settlement processing result sent to the store server 11. The store server 11 receives the aforementioned settlement processing result, and attests a settlement processing result using the key for attestation child verification beforehand exchanged with the attestation child contained there. Unless the user can know the key which had the key exchanged between the store server 11 and the settling server 13, it is impossible to forge an attestation child and forgery of a settlement processing result can be detected.

[0044]Next, again with reference to drawing 1, the composition of an electronic clearing system is explained again. The electronic clearing system shown in drawing 1 takes the next composition from a point of the function with which each terminal and a server are provided. That is, the electronic clearing system is provided with the user terminal 12 mutually connected with the channels 14, 15, and 16, the store server 11, and the settling server 13. And the settling server 13 is connected with the financial institution host machine 17.

[0045]A user terminal is provided with the following.

A means 12A to send an article or the order demand of service to said store server 11 using the channel 15 according to a user's operation.

A means 12B to receive the payment processing demand from the store server 11, and to send the 2nd settlement request to the settling server 13.

[0046]The store server 11 is provided with the following.

A means 11A to send the 1st settlement request to the settling server 13 when an order demand is received.

A means 11B to send a payment processing demand to a user terminal.

[0047]If said 1st settlement request and said 2nd settlement request are received, said settling server compared the contents of said 1st settlement request, and the contents of said 2nd settlement request, and when there is no mismatching, it is provided with the settlement processing means 13A which performs settlement processing with said financial institution host machine.

[0048]And a settling server is provided with a means 13B to send the result of said settlement processing to said user terminal 12, in a 1st embodiment, When the user terminal 12 received said settlement processing result, it was provided with a means 12C to send a settlement processing result to said store server from the user terminal 12, and the store server 11 is provided with a means 11C to receive said settlement

processing result. Processing shown in drawing 2 and drawing 3 is performed by this composition.

[0049]<A 2nd embodiment>, next a 2nd embodiment of this invention are described in detail with reference to drawings. A 2nd embodiment of this invention differs from a 1st embodiment in that the method of returning a settlement processing result to the store server 21 returns to the store server 21 from the settling server 23 directly rather than that returns to the store server 21 via the user terminal 22 from the settling server 23.

[0050]Drawing 7 is a block diagram showing the example of composition of a 2nd embodiment. The composition of the store server 21 in a 2nd embodiment, the user terminal 22, the settling server 23, the channel 24 or the channel 26, and the financial institution host machine 27 and each required function are the same except for a 1st embodiment and the following point. It is having a function the settling server 23 sending a settlement processing result to the store server 21 via the channel 24, and a function the store server 21 receiving a settlement processing result from the settling server 23 via the channel 24.

[0051]Next, operation of a 2nd embodiment is explained with reference to drawing 8 and drawing 9. In the example shown in drawing 8 and drawing 9, processing is continuing by the numerals Ba, Bb, and Bc, respectively. The channel 25 and the channel 26 presuppose that it is the Internet, and use the user terminal 22 as the terminal equipment which has a browser function of the Internet also here. Drawing 8 until a settling server performs settlement processing, and Step B1 to the step B18 of drawing 9 is the same as Step A1 to that [B18] of a 1st embodiment.

[0052]After settlement processing (Step B18) finishes, the settling server 23 returns a settlement processing result to the store server 21 first (Step B19). This is realizable if methods, such as POST of an HTTP protocol, are used. Or it is realizable also when the settling server 23 takes out an E-mail to the store server 21.

[0053]The store server 21 receives the above-mentioned settlement processing result (Step B20), if needed, if settlement of accounts is accepted, it will process shipping products to an order, etc., and if settlement of accounts is not accepted, it processes a stop, reclaim, etc. of settlement of accounts. This is realizable by the CGI script in the store server 21, etc.

[0054]When it is with methods, such as POST of an HTTP protocol, in the above-mentioned step 19, the store server 11 which received the settlement processing result sends that it has received as a response to the settling server 23 (Step B21), and the settling server 23 receives this (Step B22). However, when an

E-mail is used in Step 19, Step B21 and Step 22 are unnecessary.

[0055]Subsequently, the settling server 23 transmits a settlement processing result to the user terminal 22 (Step B23). This is realizable by returning a HTML screen as a response of the 2nd settlement request sent by methods, such as POST of an HTTP protocol. The user terminal 22 receives and (Step B24) displays this screen (Step B25).

[0056]In this 2nd embodiment, it is different at the point which a settling server is provided with a means 23C to send the result of said settlement processing to said store server, as compared with the composition shown in drawing 1, and is provided with a means 21D by which a store server receives said settlement processing result. It does not have the means shown with the numerals 11C and 12C of drawing 1.

[0057]<A 3rd embodiment>, next a 3rd embodiment of this invention are described in detail with reference to drawings. The method of returning a settlement processing result does not return a 3rd embodiment of this invention to the store server 31 from the settling server 33 via the user terminal 32 to the store server 31, The store server 31 asks the settling server 33 a settlement processing result, and the settling server 33 which received this differs from a 1st embodiment in that a settlement processing result is returned to the store server 31.

[0058]Drawing 10 is a block diagram showing the example of composition of a 3rd embodiment of this invention. The composition of the store server 31 in a 3rd embodiment, the user terminal 32, the settling server 33, the channel 34 or the channel 36, and the financial institution host machine 27 and each required function are the same except for a 1st embodiment and the following point. The function in which, as for it, the store server 31 sends an inquiry demand of a settlement processing result to the settling server 33 via the channel 34, The settling server 33 is having the function holding a settlement processing result, receiving the inquiry demand from the store server 31, and returning the demanded settlement processing result to the store server 31.

[0059]Next, operation of a 3rd embodiment is explained with reference to drawing 11 and drawing 12. In the example shown in drawing 11 and drawing 12, processing is continuing with the numerals Ca, Cb, and Cc, respectively. The channel 35 and the channel 36 presuppose that it is the Internet, and use the user terminal 32 as the terminal equipment which has a browser function of the Internet also here.

[0060]Drawing 11 until a settling server performs settlement processing, and Step C1 to the step C18 of drawing 12 is the same as Step A1 to that [C18] of a 1st embodiment.

[0061]After settlement processing (Step C18) finishes, the settling server 23 transmits a settlement processing result to the user terminal 32 (Step C19). This is realizable by returning a HTML screen as a response of the 2nd settlement request sent by methods, such as POST of an HTTP protocol. The user terminal 32 receives and (Step C20) displays this screen (Step C21). The settling server 33 shall hold a settlement processing result as fixed time and a history.

[0062]On the other hand, the store server 31 asks the settling server 33 a settlement processing result (Step C22). What is necessary is just to perform it at the fixed time lapse back, the day which received the order, scheduled time of the next day, etc., after this performs a settlement request. It is realizable if methods, such as POST of an HTTP protocol, are used.

[0063]The settling server 33 receives the inquiry from the store server 31 (Step C23). This is realizable by CGI script etc. And the history currently held is searched and the result of the asked settlement request is searched (Step C24). This search holds as a history the identification number which specifies the order included in the 1st settlement request with a settlement processing result, includes that identification number in the inquiry demand from the store server 11, and should just search a history for that identification number to a key.

[0064]The settling server 33 replies the searched settlement processing result to the store server 31 (Step C25). The store server 31 receives a settlement processing result as a response from the settling server 33 (Step C25), if needed, if settlement of accounts is accepted, it will process shipping products to an order, etc., and if settlement of accounts is not accepted, it processes a stop, reclaim, etc. of settlement of accounts.

[0065]If drawing 10 is referred to again, unlike the composition shown in drawing 1, the store server 31 is provided with a means 31E to ask said settling server the result of said settlement processing, in a 3rd embodiment. And the settling server 33 is provided with a means 33D to return the result of said settlement processing to a store server. The store server 31 is provided with a means 31F to receive the result of said settlement processing.

[0066]<Common matter of each embodiment> drawing 13 is a block diagram showing the example of general composition of the store servers 11, 21, and 31, the settling servers 13, 23, and 33, and the information processors 50A, 50B, and 50C that operate as the user terminals 12, 22, and 32. CPU51 which executes the program whose information processor constitutes an operating system from an example shown in drawing 1, and other programs, The hard disk (auxiliary storage unit) 53 which

remembered the data etc. which the program, other programs, and each program for operating systems use to be RAM52 used as the main memory of this CPU51, It has the disk drive which drives the storages 54A, such as CD-ROM. CPU stores in a hard disk etc. the program read by the disk drive 54, and reads and performs program data according to a user's operation. The information processor 50A is provided with the following.

The input parts 55, such as a keyboard.

The indicators 56, such as a display.

[0067]The information processor's 50A execution of the program for electronic banking for driving a settling server will operate it as a settling server shown in drawing 1 etc. If similarly the information processor B executes the program for electronic banking for driving a sales server, the information processor B will function as a sales server. The same may be said of a user terminal.

[0068]The program for electronic banking which operates this settling server is provided with the following.

The 1st reception command that makes the settlement request of the order concerned receive as the 1st settlement request when there is an order to said store from the user who is a holder of a user terminal (it corresponds to step A5).

The 2nd reception command that makes the settlement request of an order receive from said user terminal (it corresponds to Step A16).

Settlement request collation instructions which make the contents of said 1st settlement request, and the contents of said 2nd settlement request compare according to reception with the 1st settlement request and said 2nd settlement request (it corresponds to Step A17).

Settlement processing instructions which perform the settlement processing concerned when there is no mismatching in the contents of said 1st and 2nd settlement requests according to these settlement request collation instructions (it corresponds to Step A18).

[0069]If the information processor 50A executes the program for electronic banking for these settling servers, it will perform processing which functions as a settling server shown in drawing 1 etc., and is shown in drawing 2, drawing 3, etc.

[0070]The program for electronic banking which operates a store server is provided with the following.

Instructions to which said settling server is made to transmit as the 1st settlement

request with the identification number which identifies the order content concerned and the order concerned, and a user when an order is received from the user of a user terminal (it corresponds to step A3).

Instructions which make an order content transmit to said user terminal as a payment processing demand (it corresponds to Step A7).

Instructions which make the result of said settlement of accounts receive with the identification number which discriminates said order and a user from a settling server or said user terminal (it corresponds to Step A23, B20, and C26 grade).

[0071]The information processor's 50C execution of the program for electronic banking for operating a user terminal will operate this information processor 50C as a user terminal. The program for electronic banking for operating this user terminal is provided with the following.

The payment request instruction reception command which makes the identification number which discriminates the order content concerned concerned and the order concerned, and a user from said store server which received the order from the user of the user terminal receive as payment request instructions (it corresponds to Step A8).

2nd settlement request transmission commands that makes the 2nd settlement request for requiring settlement of the payment request concerned of said settling server according to reception of this payment request instruction reception command transmit to said settling server with the identification number of said order and a user (it corresponds to Step A15).

The settlement result reception command which makes the settlement result of the order content concerned receive from the settling server which operates according to these 2nd settlement request transmission commands (it corresponds to Step A20).

[0072]Various techniques can be taken in order to introduce each program to each information processor. The program for settling servers is stored in the storage 54A, and it may be made to introduce into an information processor via the disk drive 54 in the example shown in drawing 13. It may download from storages, such as a hard disk managed by the website (WWW server) which can download a program. When generating a html page dynamically using scripts, such as cgi, it may be made to transmit the program for electronic banking for user terminals one by one towards a user terminal from a settling server.

[0073]In a 1st embodiment, the settling server 13 is able to attest the store server 11

by using for communication between the store server 11 and the settling server 13 the correspondence procedure in which the above attestation is possible. That is, in transmission and reception of the 1st settlement request, by using the correspondence procedure which can be attested, it can check that the settling server 13 is the regular settlement request sent from the regular store server 11, and can check that the store server 11 has sent the settlement request to the regular settling server 13. The correspondence procedure in which attestation here is possible is performing the method of communicating using a dedicated line, and SSL communication using an electronic certificate etc.

[0074]Although this is the same also in a 2nd embodiment, in a 2nd embodiment, it is using the correspondence procedure which can further be attested by communication between the store server 21 and the settling server 23, and the mutual attestation with the store server 21 and the settling server 23 is possible in transmission and reception of a settlement processing result. That is, it can check that the store server 21 is the regular settlement processing result returned from the regular settling server 23, and can check that the settling server 23 has sent the settlement processing result to the regular store server 21.

[0075]This is the same as a 2nd embodiment also in a 3rd embodiment, and it can check further that the settling server 33 has received the inquiry demand of the settlement processing result from the regular store server 31 in a 3rd embodiment.

[0076]In a 1st embodiment, user authentication in a settling server and settling server attestation in a user terminal can be performed by the following methods. One method decides on the key for a user and the settling server 13 to perform an attestation child's generation and verification beforehand and the user's identifier which identifies a user first. With an attestation child here, MAC using a secret key cryptosystem (symmetrical key code), the digital signature using public key encryption, etc. are pointed out.

[0077]When the user terminal 12 sends the settlement request of the 2nd settlement request to the settling server 13, it generates the attestation child to the 2nd settlement request using the key for the aforementioned attestation child generation, and includes this attestation child and the aforementioned user's identifier in the 2nd settlement request.

[0078]In settlement processing (Step A18), the settling server 13 specifies the key for attestation child verification from the user's identifier contained in the 2nd settlement request, and performs attestation of a user and a settlement request by the attestation child to this key and the 2nd aforementioned settlement request. Thereby,

the settling server 13 can verify that it is a regular settlement request by a regular user. On the contrary, the settling server 13 includes the attestation child to a settlement processing result in the settlement processing result returned to the user terminal 12. The user terminal 12 performs attestation of the settling server 13 and a settlement processing result by the attestation child to the aforementioned settlement processing result in the reception of a settlement processing result. Thereby, the user terminal 12 can verify that it is a regular settlement processing result by the regular settling server 13.

[0079]It is between the user terminal 12 and the settling server 13 beforehand, and it is necessary to renew the key used for an attestation child's generation, and verification in the method of using the above-mentioned attestation child. What is necessary is to download the software from the settling server 13 beforehand, and just to enable it to install it in the user terminal 12 in an attestation child's generation, although software for exclusive use may be needed. This software is started by the payment processing demand from the store server 11 like the WARETTO software in SET, What is necessary is to generate and settle an attestation child, to send the 2nd settlement request to the settling server 13, to receive the settlement processing result from the settling server 13, and just to verify the attestation child as a result of the settlement request included there.

[0080]There are also a settling server and a method of using for communication between the user terminal 12 and the settling server 13 the correspondence procedure in which the above attestation is possible as an option which performs mutual recognition between users. That is, what is necessary is just to perform mutual attestation with the user terminal 12 and the settling server 13 in transmission and reception of the 2nd settlement request and a settlement processing result with the correspondence procedure which can be attested.

[0081]The user authentication in a settling server is realizable also by using ID and a password. that is, this -- beforehand -- between a user and a settling server -- a user's identifier -- the password which is user confidential information is decided to be ID, and ID and a password are included in the 2nd settlement request. The settling server 13 should just attest a user with ID and a password in settlement processing (Step A18).

[0082]The example of the above mentioned settling server and three authentication methods between user terminals is feasible also in the 2nd embodiment and 3rd embodiment.

[0083]In a 1st embodiment, user account information, such as a credit card number of

a user required for settlement processing, an account number, a password, Although it may be made to contain in the 2nd settlement request, if the user authentication by the settling server 13 is possible, it is also possible to hold a user's credit card number, an account number, etc. with the settling server 13 as mentioned above. That is, the identifier which identifies a user is included in the 2nd settlement request, and after the settling server 13 performs user authentication, if it succeeds in attestation, it searches a credit card number, an account number, etc. which held the user's identifier to the key, and should just perform settlement processing. This is the same also in the 2nd embodiment or 3rd embodiment.

[0084]According to the 1st thru/or a 3rd embodiment, the following effects are done so as mentioned above. The 1st effect is being able to keep a user's credit number and account number secret from the store side. The reason is for sending confidential information, such as a user's credit number and an account number, to a settling server directly from a user. The 2nd effect is that a user or a store cannot forge the contents of settlement of accounts. The reason is because it is able for a settling server to receive a settlement request from a user and the both sides of a store, and to compare both contents of settlement of accounts. The 3rd effect has attestation of a user and the both sides of a store possible for a settling server. The reason is because the settling server is able to attest by receiving a settlement request a user and the both sides of a store, and directly. The 4th effect eases the burden for preparing the encryption by the side of a user, the program for signature generating, and an electronic certificate. The reason is for simple consisting of a function etc. which generate an attestation child and ending with this method, also when the exclusive program or electronic certificate by the side of a user are not necessarily needed but you need them.

[0085]

[Effect of the Invention]Since this invention is constituted as mentioned above and functions, according to this, a settling server, When the 1st settlement request is received from a store server, and the 2nd settlement request is received from a user terminal, then the contents of said 1st settlement request and the contents of said 2nd settlement request are compared and there is no mismatching, in order to perform settlement processing, When the settlement request of both a store and a user is not in agreement, By making settlement processing abortive, can prevent the inaccurate settlement request by forgery, mistake, etc., and the personal information of a user required for settlement of accounts, Since accounts can be settled by comparison of an order content and the amount of money even if transmitted only

from a user terminal, The outstanding electronic account settlement method which is not in the former of it being said that a processing burden, such as giving encryption to various kinds of numbers which a user's personal information does not reveal to a store, therefore are used for a user's settlement of accounts, can be eased can be provided.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing a 1st embodiment of this invention.

[Drawing 2] It is a sequence diagram showing the preceding paragraph of operation of a 1st embodiment of this invention.

[Drawing 3] It is a sequence diagram showing the latter part of operation of a 1st embodiment of this invention.

[Drawing 4] It is an explanatory view showing the example of the screen displayed when the user terminal shown in drawing 1 orders.

[Drawing 5] It is an explanatory view showing the example of the screen displayed when a payment processing demand is made by the user terminal shown in drawing 1.

[Drawing 6] It is an explanatory view showing the example of the screen for transmitting a settlement result to a store server from the user terminal shown in drawing 1.

[Drawing 7] It is a block diagram showing a 2nd embodiment of this invention.

[Drawing 8] It is a sequence diagram showing the preceding paragraph of operation of a 2nd embodiment of this invention.

[Drawing 9] It is a sequence diagram showing the latter part of operation of a 2nd embodiment of this invention.

[Drawing 10] It is a block diagram showing a 3rd embodiment of this invention.

[Drawing 11] It is a sequence diagram showing the preceding paragraph of operation of a 3rd embodiment of this invention.

[Drawing 12] It is a sequence diagram showing the latter part of operation of a 3rd embodiment of this invention.

[Drawing 13] It is a block diagram showing the composition of the hardware resources common to each embodiment of this invention.

[Drawing 14] It is a block diagram showing the conventional electronic clearing system.

[Description of Notations]

- 11 Store server
- 12 User terminal
- 13 Settling server
- 14 Channel
- 15 Channel
- 16 Channel
- 17 Financial institution host machine
- 21 Store server
- 22 User terminal
- 23 Settling server
- 24 Channel
- 25 Channel
- 26 Channel
- 27 Financial institution host machine
- 31 Store server
- 32 User terminal
- 33 Settling server
- 34 Channel
- 35 Channel
- 36 Channel
- 37 Financial institution host machine

[Translation done.]